Mega 200VWR

USER GUIDE

visit us at
www.telkomphones.co.za
for more products

2C telecoms

www.telkom.co.za

Telkom
Touch tomorrow

Table of Contents

CHAPTER 1: INTRODUCTION 5

INTRODUCTION TO YOUR ROUTER 5
FEATURES 5

CHAPTER 2: INSTALLING THE ROUTER 8

IMPORTANT NOTE FOR USING THIS ROUTER 8
PACKAGE CONTENTS 8
THE FRONT LEDS 9
THE REAR PORTS 10
CABLING 11

CHAPTER 3: BASIC INSTALLATION 12

CONNECTING YOUR ROUTER 13
FACTORY DEFAULT SETTINGS 18
Web Interface (Username and Password) 18
Device LAN IP settings 18
ISP setting in WAN site 18
DHCP server 18
LAN and WAN Port Addresses 18
INFORMATION FROM YOUR ISP 19
CONFIGURING WITH YOUR WEB BROWSER 20

CHAPTER 4: CONFIGURATION 21

STATUS 22
ARP Table 22
Wireless Association Table 22
Routing Table 22
DHCP Table 23
PPTP Status 24
IPSec Status 24
L2TP Status 25
Email Status 25
VoIP Status 25
Event Log 26
Error Log 26
NAT Sessions 27
Diagnostic 27
UPnP Portmap 28
QUICK START 29
CONFIGURATION 31
LAN - Local Area Network 31
Bridge Interface 31
Ethernet 32
IP Alias 32
Ethernet Client Filter 33
Wireless 35
Wireless Security 37
Wireless Client / MAC Address Filter 39
Port Setting 41
DHCP Server 42

WAN - Wide Area Network ... *43*
ISP ... 43
DNS ... 53
ADSL ... 54
System ... *56*
Time Zone ... 56
Remote Access ... 57
Firmware Upgrade ... 58
Backup / Restore ... 59
Restart Router ... 60
User Management ... 61
Firewall and Access Control ... *62*
General Settings ... 63
Packet Filter ... 64
Intrusion Detection ... 72
URL Filter ... 74
IM / P2P Blocking ... 76
Firewall Log ... 77
VPN - Virtual Private Networks ... *78*
PPTP (Point-to-Point Tunneling Protocol) ... 78
IPSec (IP Security Protocol) ... 88
L2TP (Layer Two Tunneling Protocol) ... 98
VoIP - Voice over Internet Protocol ... *110*
Wizard ... 111
General Settings ... 113
Phone Port ... 116
PSTN Dial Plan ... 118
VoIP Dial Plan ... 122
Ring & Tone ... 127
Special Dial Codes ... 128
QoS - Quality of Service ... *129*
Prioritization ... 129
Outbound IP Throttling (LAN to WAN) ... 131
Inbound IP Throttling (WAN to LAN) ... 132
Virtual Server (known as Port Forwarding) ... *136*
Add Virtual Server ... 137
Edit DMZ Host ... 138
Edit DMZ Host ... 139
Edit One-to-One NAT (Network Address Translation) ... 140
Time Schedule ... *143*
Configuration of Time Schedule ... 144
Advanced ... *145*
Static Route ... 145
Dynamic DNS ... 146
Check Email ... 147
Device Management ... 148
IGMP ... 151
VLAN Bridge ... 151
SAVE CONFIGURATION TO FLASH ... 155
LOGOUT ... 156

CHAPTER 5: TROUBLESHOOTING ... 157

PROBLEMS STARTING UP THE ROUTER ... 157
PROBLEMS WITH THE WAN INTERFACE ... 157

PROBLEMS WITH THE LAN INTERFACE 157
APPENDIX A: WINDOWS 98 SETUP 158

Chapter 1: Introduction

Introduction to your Router

Your Mega 200VWR router is an “all-in-one” VoIP ADSL router, combining an ADSL 2+ modem, ADSL router, Ethernet network switch and 2 telephone ports for Voice over IP functionality, providing everything you need to get the computers on your network connected to the Internet over your ADSL connection. With features such as an ADSL Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users as well as gurus requiring advanced features and control over their Internet connection and network.

Features

- **Voice over IP Compliance with SIP Standard**
  This router supports cost-effective, toll-quality voice calls over the Internet. It complies with the most popular industrial standard, SIP protocol, to ensure the interoperability with SIP devices and major VoIP Gateways. This router supports call waiting, silence suppression, voice activity detection (VAD), comfort noise generation (CNG), line echo cancellation, caller ID (Bell 202, V3) and so on.

- **Fixed-Line Support**
  The router integrates RJ-11 FXO port for inbound and outbound calls transmitted through PSTN. Users can receive phone calls from PSTN while enjoying VoIP call service at the same time. In addition, the device has automatic fallback to the POTS line to enable making normal phone calls when there is a power outage, or when the Internet connection is down (lifeline function).

- **Express Internet Access**
  This router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users can enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis.plus (ITU G.992.5)).

- **Virtual Private Network (VPN)**
  This function allows user to make a tunnel with a remote site directly to secure the data transmission among the connection. Users can use the embedded PPTP and L2TP client/server, IKE and IPSec, which are supported by this router to make a VPN connection, or users can run a PPTP client on a computer. if the user runs a PPTP client on his local computer, the router will provide a IPSec and PPTP pass through function to establish the VPN connection

- **802.11g Wireless AP with WPA Support**
  With the integrated 802.11g Wireless Access Point, the router offers quick and easy access between the wired network, wireless network and ADSL connection with single device simplicity, and as a result, mobility to the users. The wireless AP supports 54 Mbps 802.11g data connections, and is backward compatible with existing 802.11b equipment. The Wireless Protected Access (WPA1 and WPA2) and Wireless Encryption Protocol (WEP) features enhance wireless security and provide access control..

- **Fast Ethernet Switch**
  A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.

- **Multi-Protocol to Establish a Connection**
  This router supports PPPoA, RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet and IPoA to establish a connection with the ISP. It also supports VC-based and LLC-based multiplexing.

- **Quick Installation Wizard**
  The router has a WEB GUI page to allow quick installation of the router. With this wizard, end users can enter their ISP information easily and quickly, and surf the Internet immediately.

- **Universal Plug and Play (UPnP) and UPnP NAT Traversal**
  This protocol is used to enable simple and robust connectivity among stand-alone devices and computers from many different vendors. It makes networking simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to applications such as Net Meeting or MSN Messenger seamlessly.

- **Network Address Translation (NAT)**
  This function allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateways (ALG) are supported, such as web browsing, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

- **SOHO Firewall Security with DoS and SPI**
  Along with the built-in NAT natural firewall feature, the router also provides advanced hacker pattern-filtering protection. It can automatically detect and block Denial of Service (DoS) attacks. The router is built with Stateful Packet Inspection (SPI) to determine if a data packet is allowed through the firewall to the LAN.

- **Domain Name System (DNS) Relay**
  This provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) to an IP address. When a local computer has its DNS server IP address configured to the router's IP address, every DNS conversion request packet from the Computer to this router will be forwarded to the real DNS in the outside network.

- **Dynamic Domain Name System (DDNS)**
  The Dynamic DNS service allows you to alias a dynamic WAN IP address to a static hostname. To use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 different DDNS servers are supported.

- **Quality of Service (QoS)** QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, or port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

- **Virtual Server ("port forwarding")**
  Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN to act as a WEB server and expose it to Internet users. Outside users can browse this web server directly, while it is still protected by NAT. A DMZ host setting is also provided to completely expose a local computer the Internet.

- **Rich Packet Filtering**
  This not only filters the packet based on IP address, but also based on Port numbers. It will filter

packets to and from the Internet, and provides a higher level of security control.

- **Dynamic Host Configuration Protocol (DHCP) Client and Server**
  On the WAN interface, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. On the LAN interface, the DHCP server can allocate a range of client IP addresses and distribute them, including IP address, subnet mask as well as DNS IP address, to local computers. This provides an easy way to manage the local IP network.

- **Static and RIP1/2 Routing**
  It has routing capability and supports a static routing table or RIP1/2 routing protocol.

- **Simple Network Management Protocol (SNMP)**
  This is an easy way to remotely manage the router via SNMP.

- **Web based GUI**
  The routers' web based GUI is used for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage the router. .

- **Firmware Upgradeable**
  This router can be upgraded to the latest firmware through the WEB based GUI.

- **Rich Management Interfaces**
  This router supports flexible management interfaces using a local console, LAN or WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

Chapter 2: Installing the Router

Important note for using this router

Warning

- ✓ **Do not use this router in high humidity or high temperatures.**
- ✓ **Do not use the same power source for this router and other equipment.**
- ✓ **Do not open or repair the case yourself. If this router is too hot, turn off the power immediately and have it repaired at a qualified service center.**
- ✓ **Avoid using this product and its accessories outdoors.**

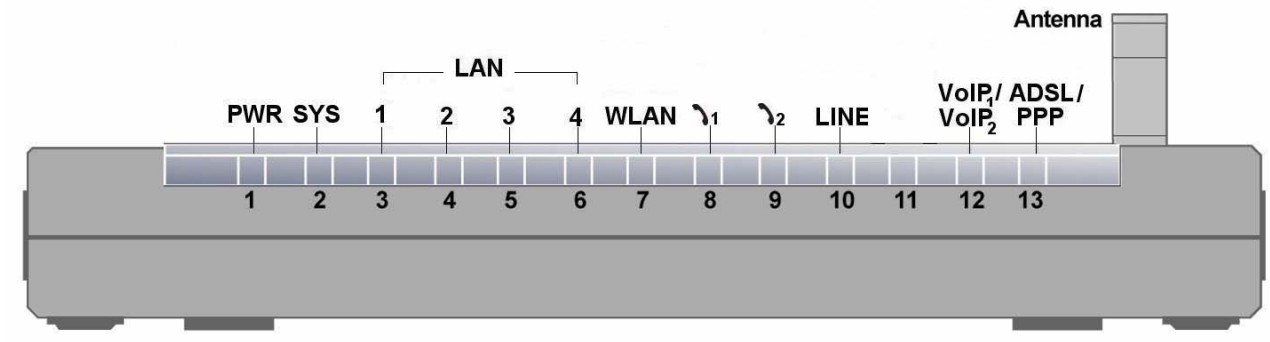
Attention

- ✓ **Place this router on a stable surface.**
- ✓ **Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage this router.**

Package Contents

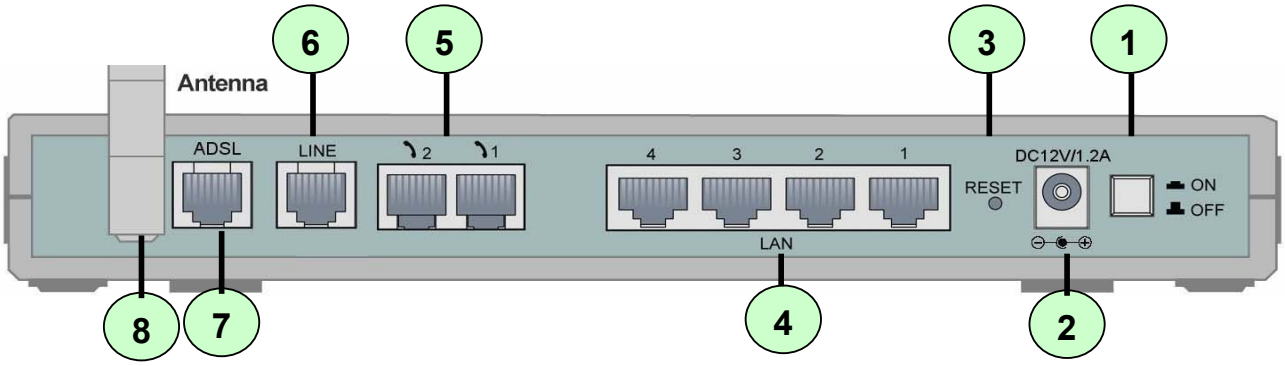
- Mega 200VWR Router
- CD-ROM containing this online manual
- RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5 LAN) Cable
- Console tool kit
- AC-DC power adapter (12VDC, 1.2A)
- A detachable antenna
- Two Micro filters
- Quick Start Guide

The Front LEDs



LED		Meaning
1	**PWR**	Lit when power is ON.
2	**SYS**	Lit when the system is ready.
3 – 6	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps. Blinking when data is Transmitted / Received.
7	**WLAN**	Green when the wireless connection is established. Flashing when sending/receiving data.
8 – 9	**Phone** **1X — 2X** (RJ-11 connector)	Green when the phone is off-hook.
10	**LINE**	Lit when inbound and outbound calls are using the PSTN.
12	**VoIP Port** **1X — 2X** (RJ-11 connector)	Lit when the SIP Registration is OK. Green for Phone 1; Orange for Phone 2. Note: Also orange when both Phone 1 and 2 are registered OK at the same time.
13	**ADSL/PPP**	Green when successfully connected to an ADSL DSLAM, ("line synch"). Orange when there is a PPPoA / PPPoE connection.

The Rear Ports



NOTE: **The Ethernet Port # 4 can be used as a console port. You need a special console tool which is included in the package, to connect between LAN port 4 and a PC's RS-232 port (9-pin serial port).**

Port		Meaning
1	**Power Switch**	Power ON/OFF switch
2	**PWR**	Connect the supplied power adapter to this jack.
3	**RESET**	When the router is turned on → the reset button is used to: Reset the router: press for **1-3 seconds**: Restore factory default settings: press for more than **6 seconds, and power cycle the router**: (useful if you cannot login to the router or have forgotten your Username/Password.). **Caution**: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device.
4	**LAN** **1X — 4X** (RJ-45 connector)	To connect your router to a PC or an office/home network of 10Mbps or 100Mbps use a UTP Ethernet cable (Cat-5 or Cat-5e) and connect to one of the LAN ports. **Caution**: Port 4 can be either a LAN or a Console port at any time but not simultaneously.
4	**Console Port (LAN port 4)** (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to LAN Port 4 and connect to the computers RS-232 port via the supplied adaptor. **Caution**: Port 4 can be either a LAN or a Console port at any time but not simultaneously
5	**Phone** **1X — 2X** (RJ-11 connector)	When using the VoIP functions, connect an analog phone to this port using a RJ-11 cable.
6	**LINE**	When using the VoIP functions, use a RJ-11cable to connect this port to the telephone wall jack..

7	**ADSL**	Use the supplied RJ-11 (“telephone”) cable to connect this port to the ADSL/telephone wall jack .
8	**Antenna**	Connect the detachable antenna to this port.

Cabling

One of the most common causes of ADSL problems is bad cabling or ADSL lines. Make sure that all devices connected to your telephone line are turned on, and that all telephones used on the line are connected via micro filters.. On the front of the product is a bank of LEDs. Once you have installed you router, verify that the LAN Link and ADSL line LEDs are lit. If they are not, check that you are using the proper/functional cables.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket, and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Chapter 3: Basic Installation

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me, etc. The product provides an easy and user-friendly interface for configuration.

Please check your Computer's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your operating system manuals.

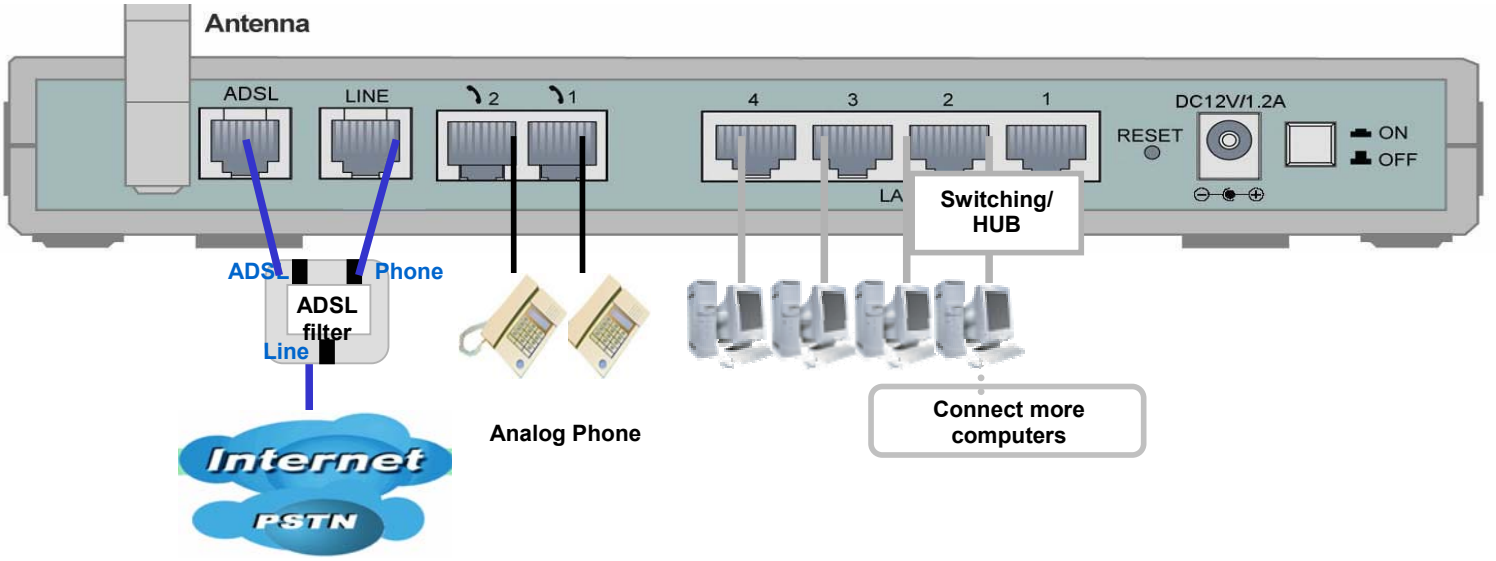
You can connect your computer to the router either through an external hub/switch or directly. However, please ensure that your computer has a properly installed Ethernet interface prior to connecting it to the router. You ought to configure your Computers to obtain an IP address through a DHCP server or you can set them up with a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **10.0.0.2** and the subnet mask is **255.255.255.0** (i.e. any attached Computer must be in the same subnet, and have an IP address in the range of 10.0.0.1 to10.0.0.254). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router's web interface it may also be advisable to temporarily remove any kind of software firewall on your Computer's as they can cause problems accessing the 10.0.0.2 IP address of the router. Users should always make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation.

Any TCP/IP capable workstation can be used to communicate with or through the router. To configure other types of workstations, please consult the manufacturer's documentation.

Connecting Your Router

1. Connect this router to a **LAN** (Local Area Network) and the ADSL/telephone (**ADSL**) network.
2. Power on the device.
3. Make sure the **PWR** and **SYS** LEDs are lit steadily and that the **LAN** LED is lit.
4. Connect an RJ11 cable to VoIP port when connecting to an analog phone set.
5. Connect RJ-11 cable to LINE Port when connecting to the telephone wall jack.



Configuring PCs in Window XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click **Network Connections**.
2. Double-click **Local Area Connection**. **(See Figure 3.1)**

Figure 3.1: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. (**See Figure 3.2)**

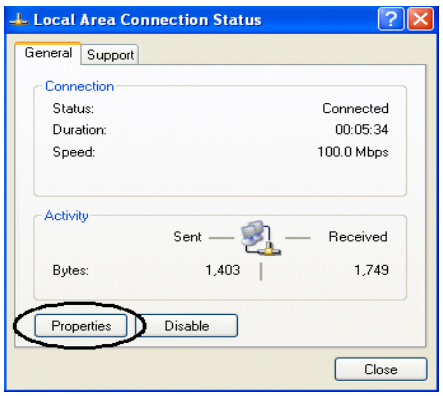


Figure 3.2: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. (**See Figure 3.3)**

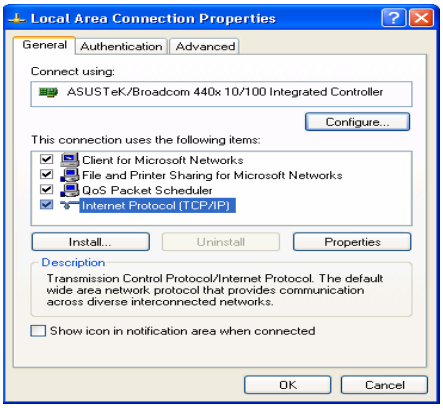

Local Area Connection Properties
General Authentication Advanced
Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

Figure 3.3: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (**See Figure 3.4**)
6. Click **OK** to finish the configuration.

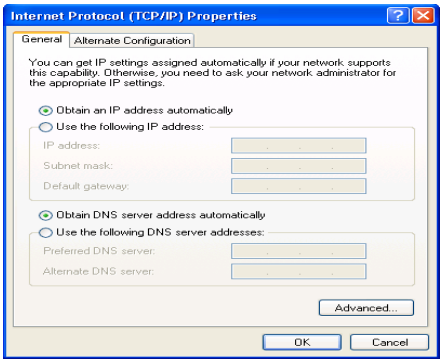

Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

Figure 3.4: IP Address & DNS Configuration

Configuring PCs in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network and Dial-up Connections**.
2. Double-click **Local Area ("LAN") Connection**. **(See Figure 3.5)**

Figure 3.5: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. **(See Figure 3.6)**

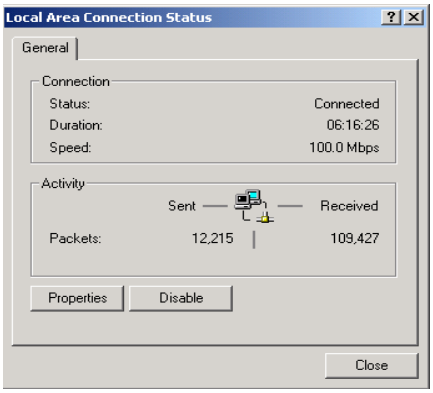


Figure 3.6: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. **(See Figure 3.7)**

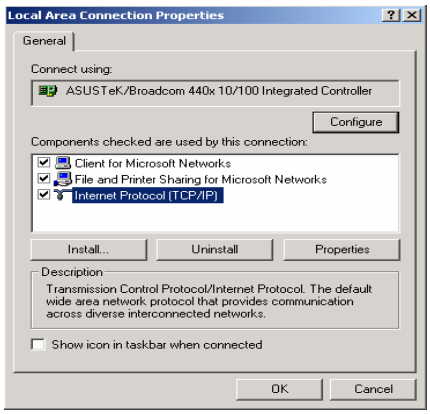


Figure 3.7: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. **(See Figure 3.8)**
6. Click **OK** to finish the configuration.

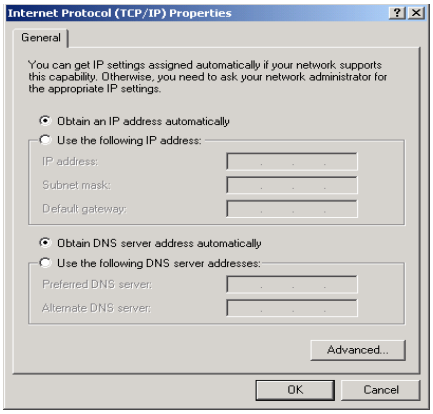

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3.8: IP Address & DNS Configuration

Configuring PC in Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of the Network Interface Card (NIC) in your PC. (**See Figure 3.9)**
3. Click **Properties**.

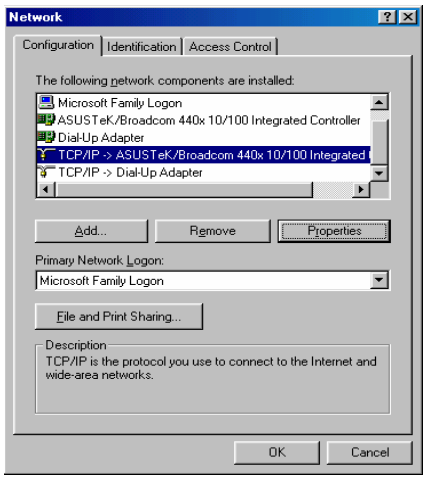


Figure 3.9: TCP / IP

4. Select the **IP Address** tab. In this page, click the Obtain an IP address automatically radio button. (**See Figure 3.10)**

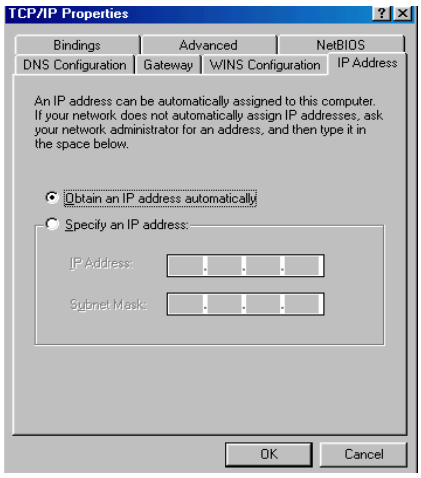

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Figure 3.10: IP Address

5. Then select the **DNS Configuration** tab. **(See Figure 3.11)**
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

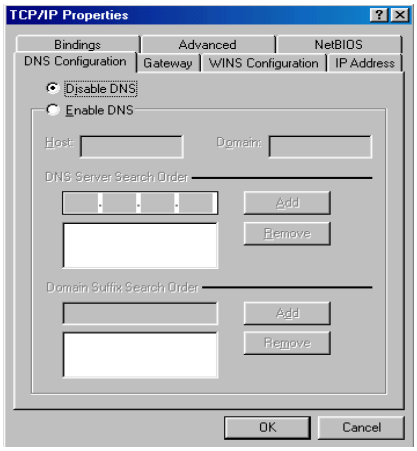


Figure 3.11: DNS Configuration

Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**. (**See Figure 3.12)**

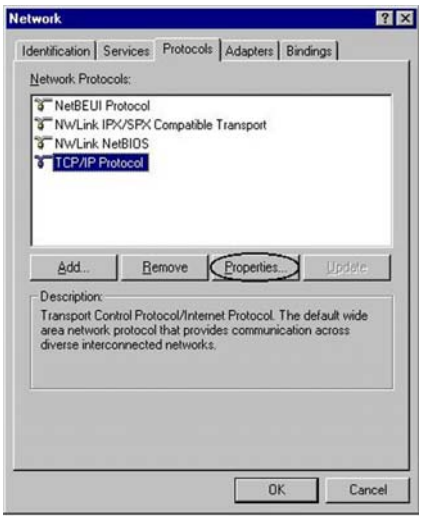


Figure 3.12: TCP / IP

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**. (**See Figure 3.13)**

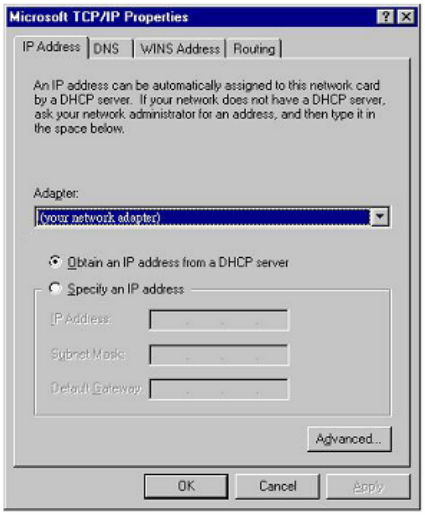

Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Figure 3.13: IP Address

Factory Default Settings

Before configuring your, you need to know the following default settings.

Web Interface (Username and Password)

- Username: admin
- Password: admin

The default username and password are "**admin**" and "**admin**" respectively.

If you ever forget the username/password to login to the router, you may press the RESET button for more than 6 seconds to restore the factory default settings.
Caution: After pressing the RESET button for more than 6 seconds, be sure you power cycle the device again.

Device LAN IP settings

- IP Address: 10.0.0.2
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

- DHCP server is enabled.
- Start IP Address:10.0.0.100
- IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	10.0.0.2	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 10.0.0.100 through 10.0.0.199	

Information from your ISP

Telkom ADSL connections use PPPoE, and automatically assign a WAN IP address to your router; The following information is provided should you wish to connect to an alternative ISP. .

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (this is automatically set by the Telkom network but be set manually should this be required).
PPPoE / PPPoE with Pass-through	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (this is automatically set by the Telkom network but be set manually should this be required). In addition, additional WAN address can be assigned using PPPoE dialer.
PPPoA	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually).
RFC 1483 Bridged	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.
RFC 1483 Routed	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA Routed (IP over ATM)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **10.0.0.2**, and click "**Go**", a user name and password window prompt will appear. **The default username and password are "admin" and "admin"** respectively**. (See Figure 3.14)**

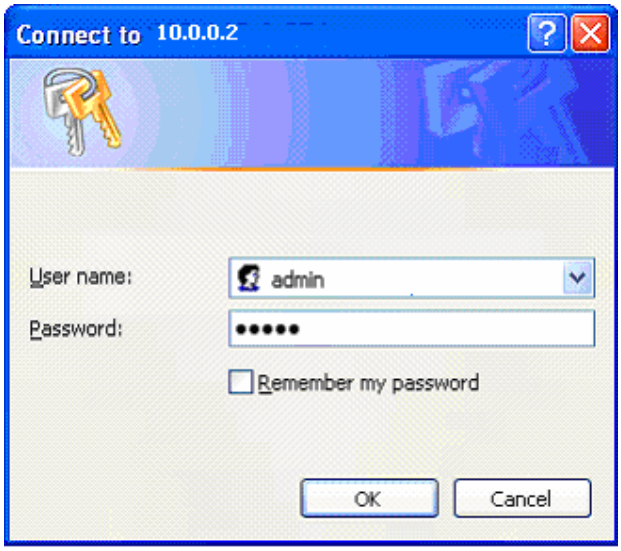


Figure 3.14: User name & Password Prompt Widonw

Congratulation! You are now successfully logged on to your Router!

Chapter 4: Configuration

On the configuration homepage, the left navigation pane, where bookmarks are provided, links you directly to the various setup pages, including:

- **Status**
  - ARP Table
  - Wireless Association
  - Routing Table
  - DHCP Table
  - PPTP Status
  - IPSec Status
  - L2TP Status
  - Email Status
  - VoIP Status
  - Event Log
  - Error Log
  - NAT Sessions
  - Diagnostic
  - UPnP Portmap
- **Quick Start**
- **Configuration**
  - LAN
  - WAN
  - System
  - Firewall
  - VPN
  - VoIP
  - QoS
  - Virtual Server
  - Time Schedule
  - Advanced
- **Save Config to FLASH**
- **Language** (provides user interface in English and French languages)
- **Logout**

Please click the links to see the relevant sections of this manual for detailed instructions on how to configure this Router.

Status

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs when you wish to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.

ARP Table

IP <> MAC List

IP Address	MAC Address	Interface	Static
10.0.0.100	00:02:3f:69:d1:67	iplan	no

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

MAC Address: The MAC (Media Access Control) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

- "**no**" for dynamically-generated ARP table entries.
- "**yes**" for static ARP table entries added by the user.

Wireless Association Table

Wireless Association Table

Wireless client's MAC address and the corresponding IP address

IP Address

IP Address: It is IP address of wireless clients that join this network.

MAC: The MAC address of wireless client.

Routing Table

Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost
✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	1

RIP Routing Table

Destination	Netmask	Gateway	Cost
0.0.0.0	0.0.0.0	0.0.0.0	1

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination IP networks ' Netmask.

Gateway/Interface: The IP address of the gateway, or existing interface, that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table

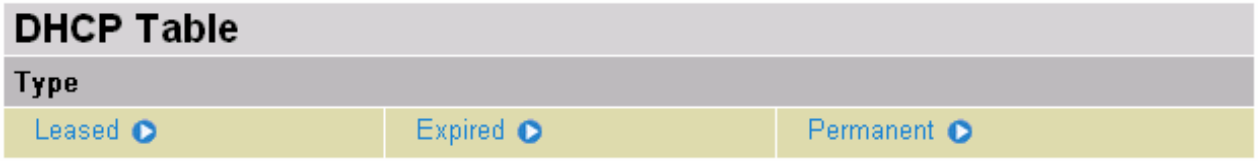
Destination: The IP address of the destination network.

Netmask: The destination IP networks ' Netmask .

Gateway: The IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

DHCP Table



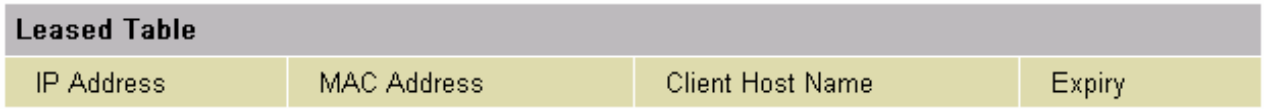
Leased: The DHCP assigned IP addresses information.

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

Leased Table



IP Address: The IP address that is assigned to a client.

MAC Address: The MAC address of the client.

Client Host Name: The Host Name (Computer Name) of the client.

Expiry: The current lease time of clients IP address.

Expired Table

Please refer the **Leased Table**.

Permanent Table

Name: The name you assigned to the Permanent configuration.

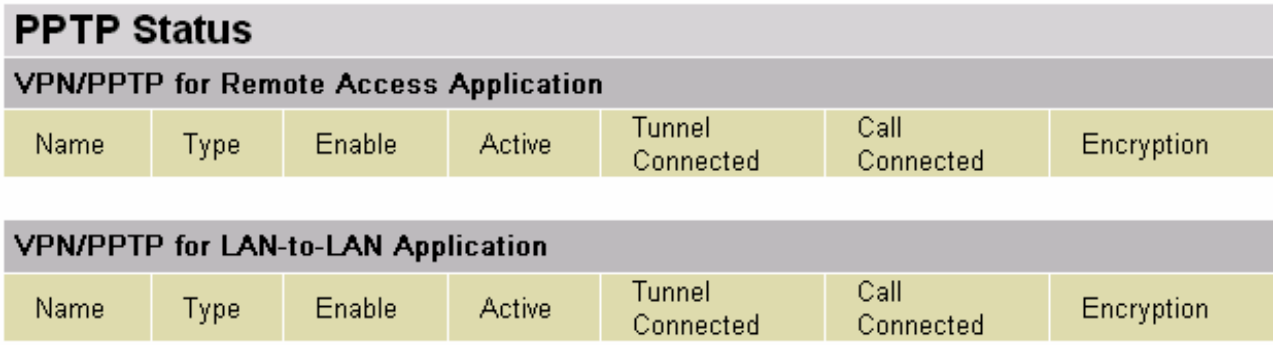
IP Address: The fixed IP address for the specific client.

MAC Address: The MAC Address that you want to assign the fixed IP address.

Maximum Lease Time: The maximum lease time interval you allow to this client.

PPTP Status

This shows details of your configured PPTP VPN Connections.



PPTP Status

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/PPTP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular PPTP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

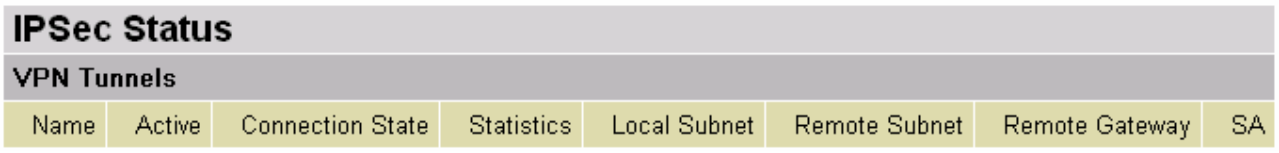
Tunnel Connected: Whether the VPN Tunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

IPSec Status

This shows details of your configured IPSec VPN Connections.



IPSec Status

VPN Tunnels

Name	Active	Connection State	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA

Name: The name you assigned to the particular VPN entry.

Active: Whether the VPN Connection is currently Active.

Connection State: Whether the VPN is Connected or Disconnected.

Statistics: Statistics for this VPN Connection.

Local Subnet: The local IP Address or Subnet used.

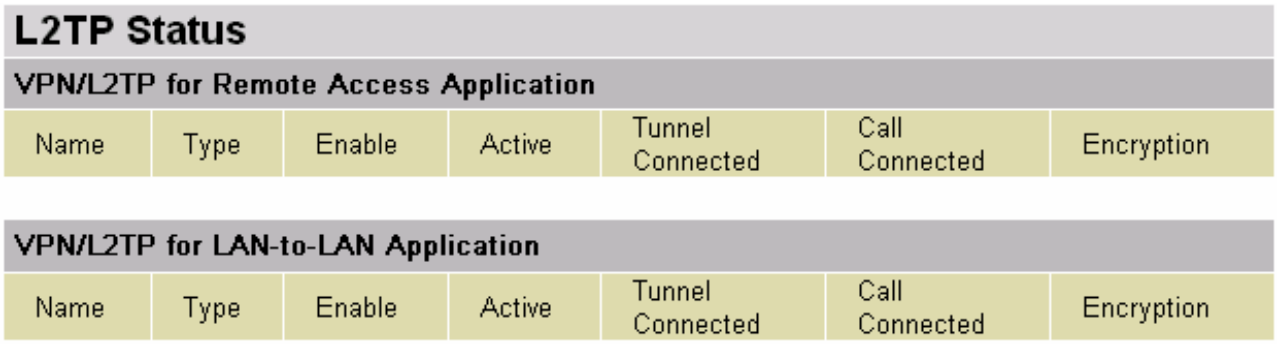
Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

L2TP Status

This shows details of your configured L2TP VPN Connections.



L2TP Status

VPN/L2TP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/L2TP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular L2TP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

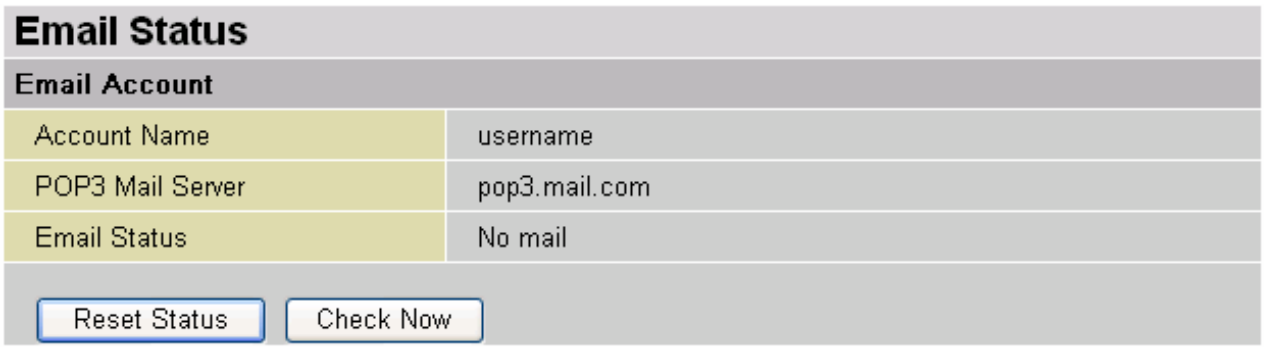
Tunnel Connected: Whether the VPN Tunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

Email Status

Details and status for the Email Account you have configured the router to check. Please see the **Advanced** section of this manual for details on this function.



Email Status

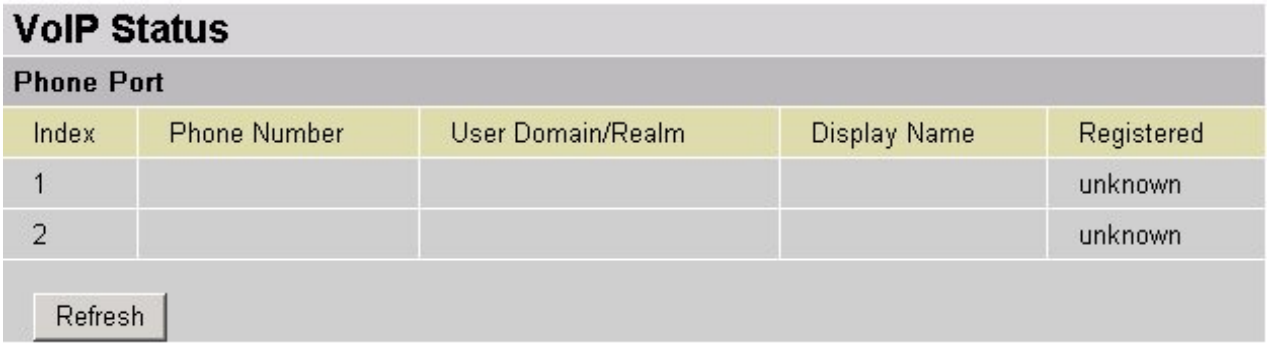
Email Account

Account Name	username
POP3 Mail Server	pop3.mail.com
Email Status	No mail

Reset Status | Check Now

VoIP Status

Here you can check details and status of VoIP Account you have configured. Please see the **VoIP Configuration** section for more details.



VoIP Status

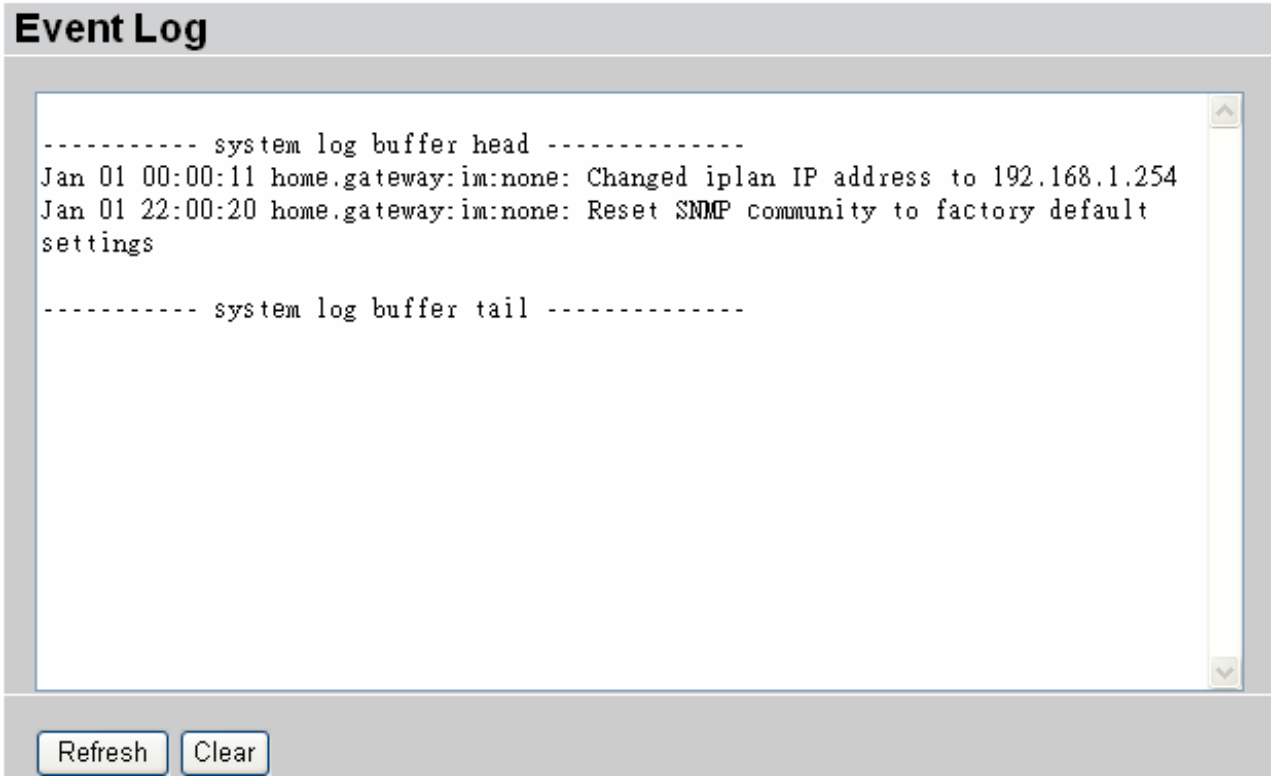
Phone Port

Index	Phone Number	User Domain/Realm	Display Name	Registered
1				unknown
2				unknown

Refresh

Event Log

This page displays the router's Event Log entries. Major events are logged to this window, such as when the router's ADSL connection is disconnected, as well as Firewall events when you have enabled Intrusion or Blocking Logging in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.

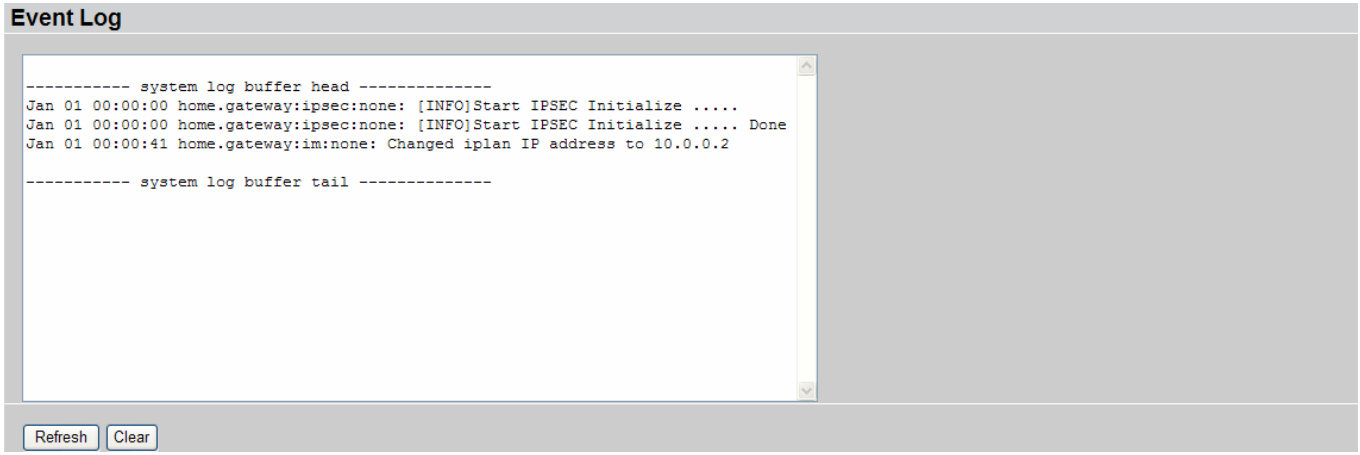

Event Log
---------- system log buffer head --------------
Jan 01 00:00:11 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 01 22:00:20 home.gateway:im:none: Reset SNMP community to factory default settings
---------- system log buffer tail --------------
Refresh
Clear

Error Log

Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.

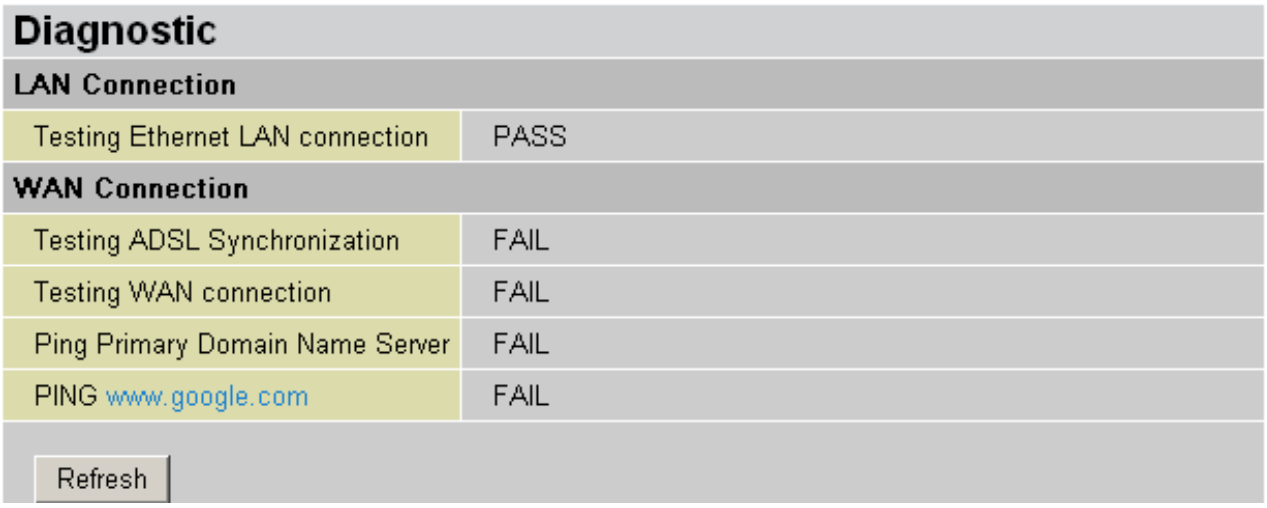
NAT Sessions

This section lists all current NAT sessions between interface of types external (WAN) and internal (LAN).


Event Log
---------- system log buffer head --------------
Jan 01 00:00:00 home.gateway:ipsec:none: [INFO]Start IPSEC Initialize .....
Jan 01 00:00:00 home.gateway:ipsec:none: [INFO]Start IPSEC Initialize ..... Done
Jan 01 00:00:41 home.gateway:im:none: Changed iplan IP address to 10.0.0.2
---------- system log buffer tail --------------
Refresh
Clear

Diagnostic

It tests the connection to computer(s) which is connected to LAN ports and also the WAN Internet connection. If **PING** **www.google.com** shows FAIL and the rest show PASS, you ought to check that your Computers' DNS settings are correctly set.



UPnP Portmap

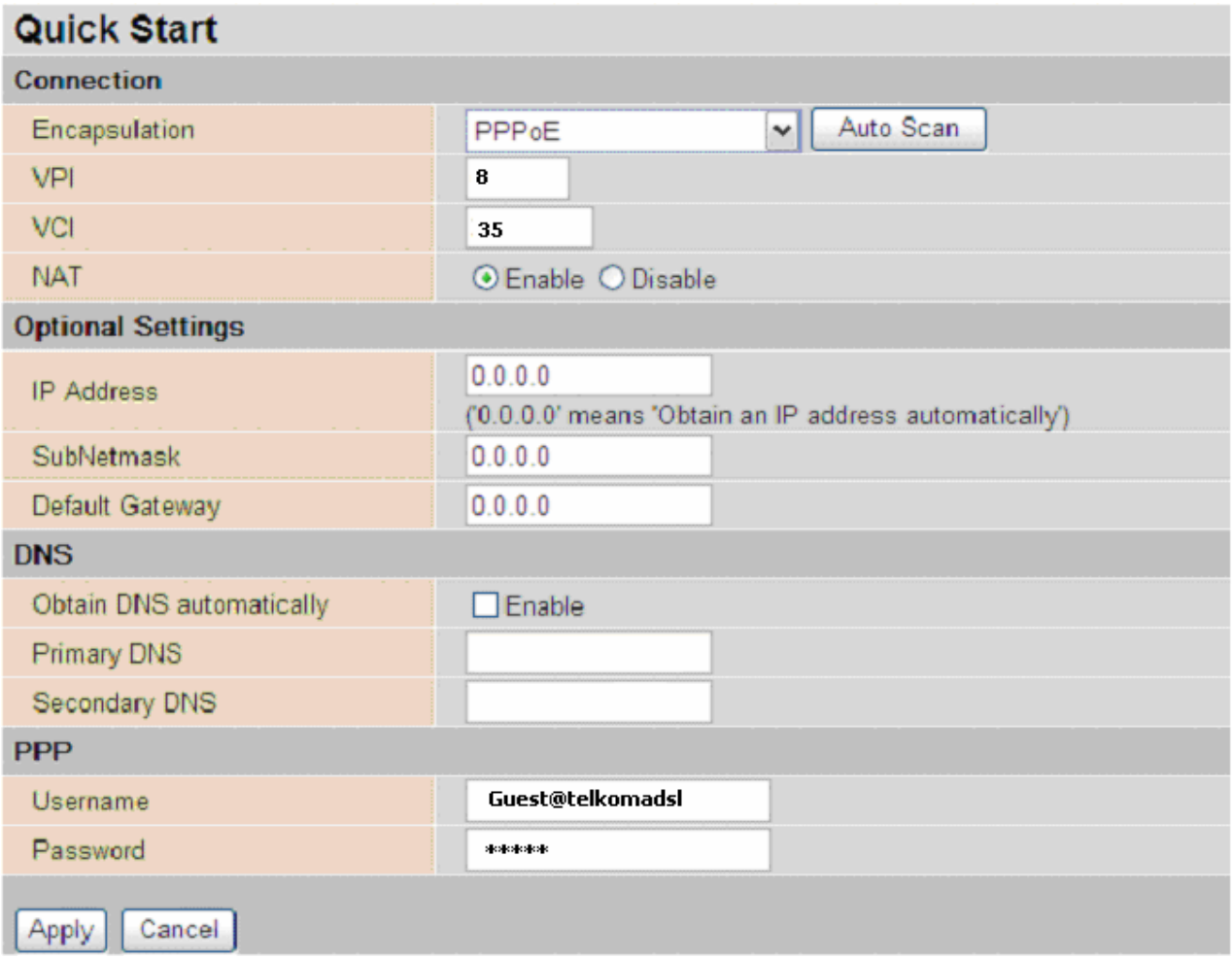
The section lists all port-mappings established using UPnP (Universal Plug and Play). See the **Advanced** section of this manual for more details on UPnP and the router's UPnP configuration options.

UPnP Portmap

UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address
emwebigd1024	udp	35324 ~ 35324	15852 ~ 15852	192.168.1.205
emwebigd1025	tcp	48888 ~ 48888	14811 ~ 14811	192.168.1.205
emwebigd1063	udp	9210 ~ 9210	15169 ~ 15169	192.168.1.202
emwebigd1064	tcp	50937 ~ 50937	14500 ~ 14500	192.168.1.202

Quick Start

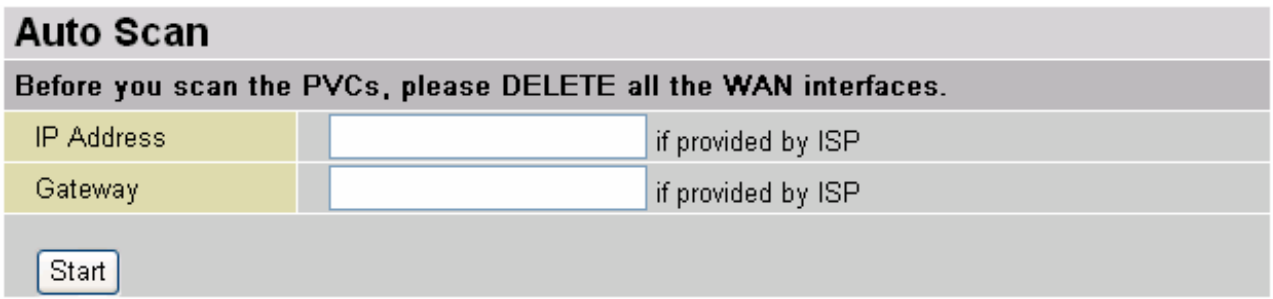


While it is recommended that you use the installation utility that was supplied with your router, It is also possible you use the built-in Quick Start function in order to configure your router.

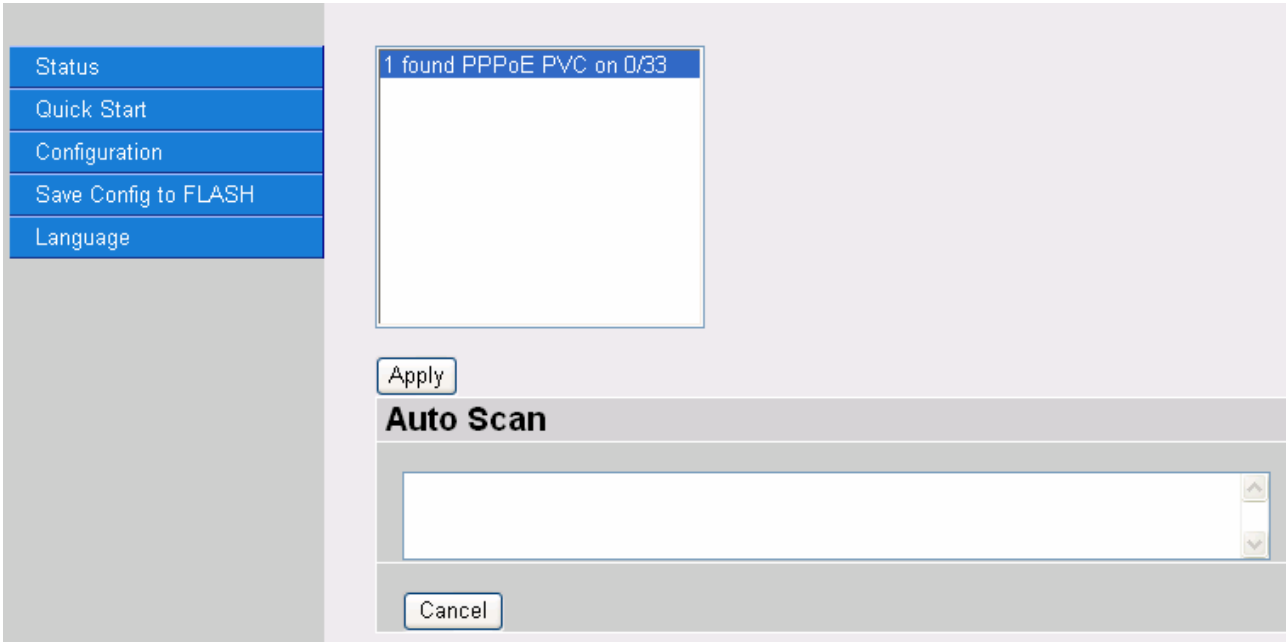
For detailed instructions on configuring your WAN settings, please see the **WAN** section of this manual.

Usually, the only details you will need for the Quick Start wizard to get you online are your login (often in the form of *username@ispname*), your password and the encapsulation type. (For the Telkom network, VCI and VPI are 8 and 35) In additional, you have the option to provide specific DNS if you desire, or select the **Enable** box to get an DNS automatically assigned by your ISP.

Your ISP will be able to supply all the details you need, alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to attempt to determine the Encapsulation types offered by your ISP.



Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful you will then be presented with a list of supported options:



Select the desired option from the list and click **Apply** to return to the Quick Start interface to continue configuring your ISP connection. Please note that the contents of this list will vary, depending on what is supported by your ISP.

Configuration

When you click this item, you will be able to following sub-items to configure the ADSL router.

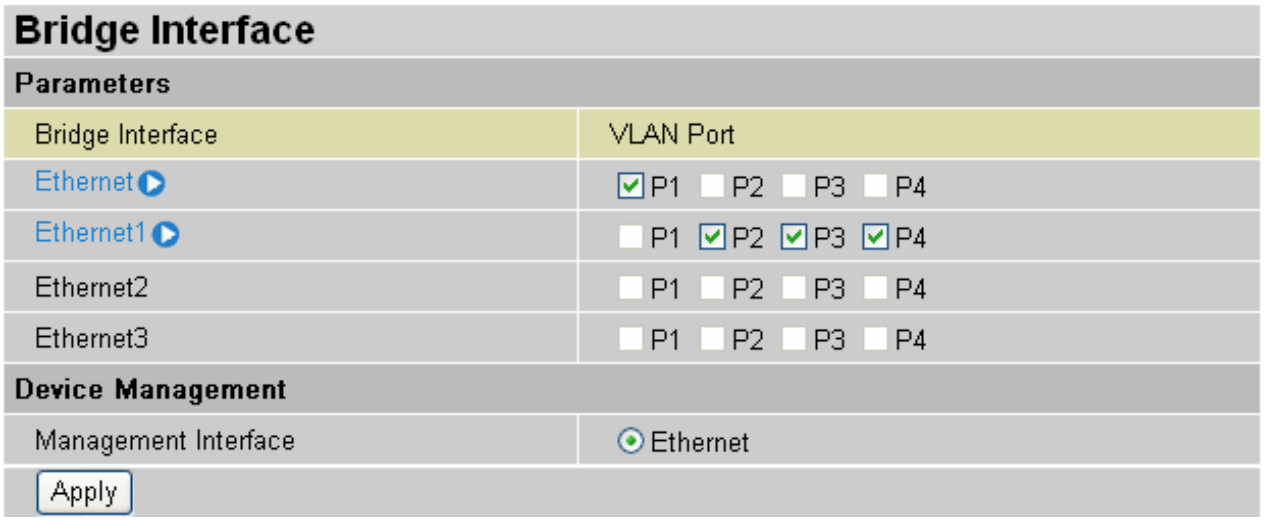
- **LAN, Wan, System, Firewall, VPN, VoIP, QoS, Virtual Server, Time Schedule** and **Advanced**

These functions are described below in the following sections.

LAN - Local Area Network

Here are the items within the LAN section: **Bridge Interface, Ethernet, IP Alias, Ethernet Client Filter, Wireless, Wireless Security, Wireless Client Filter, Port Settings** and **DHCP Server**.

Bridge Interface



You can setup member ports for each VLAN group under Bridge Interface section. From the example, two VLAN groups need to be created.

Ethernet: P1 (Port 1)

Ethernet1: P2, P3 and P4 (Port 2, 3, 4). Uncheck P2, P3, P4 from Ethernet VLAN port first.

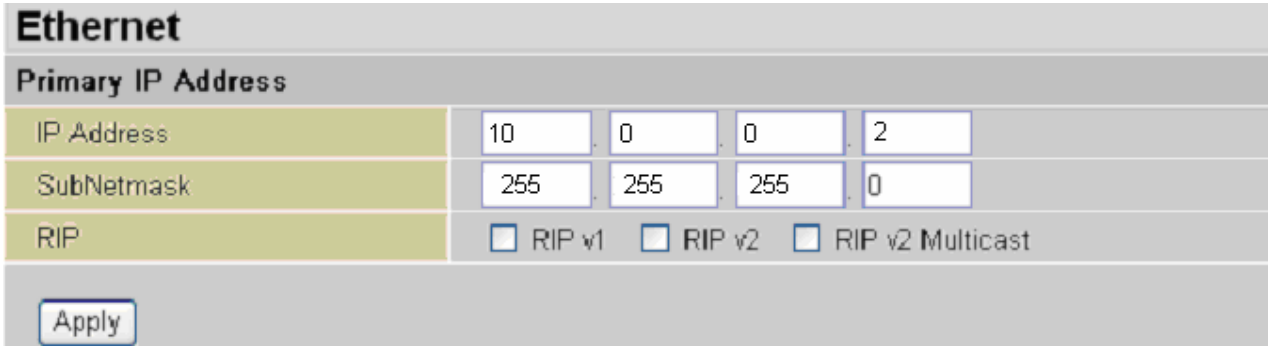
Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4

Management Interface: To specify which VLAN group is allowed to do device management - i.e web management.

Note: NAT/NAPT can be applied to management interface only.

Ethernet



Primary IP Address

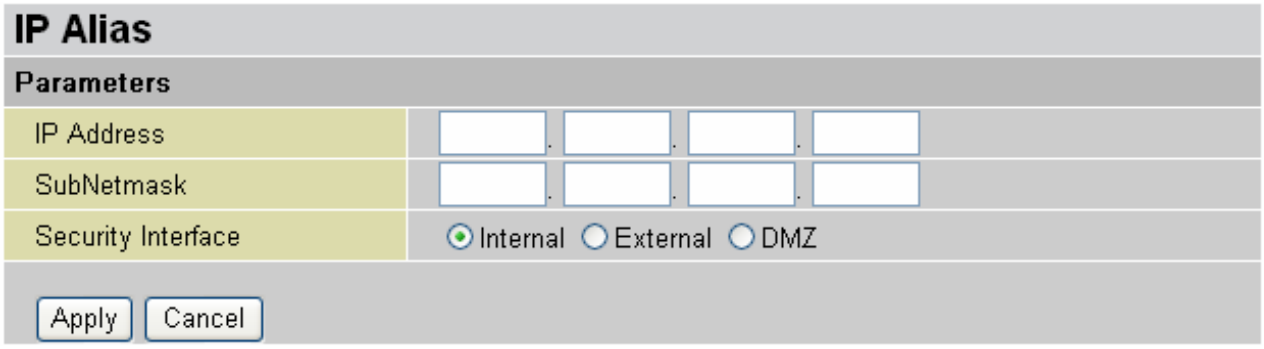
IP Address: The default IP on this router.

SubNetmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

IP Alias

This function supports to create multiple virtual IP interfaces on this router. this helps if you wish to connect two or more local networks using different IP ranges to internet via the router. In this case, an additional internal router is not required.



IP Address: Specify an IP address on this virtual interface.

SubNetmask: Specify a subnet mask on this virtual interface.

Security Interface: Specify the firewall setting on this virtual interface.

Internal: The network is behind NAT. All traffic will do network address translation (NAT) when sending out to Internet (if NAT is enabled).

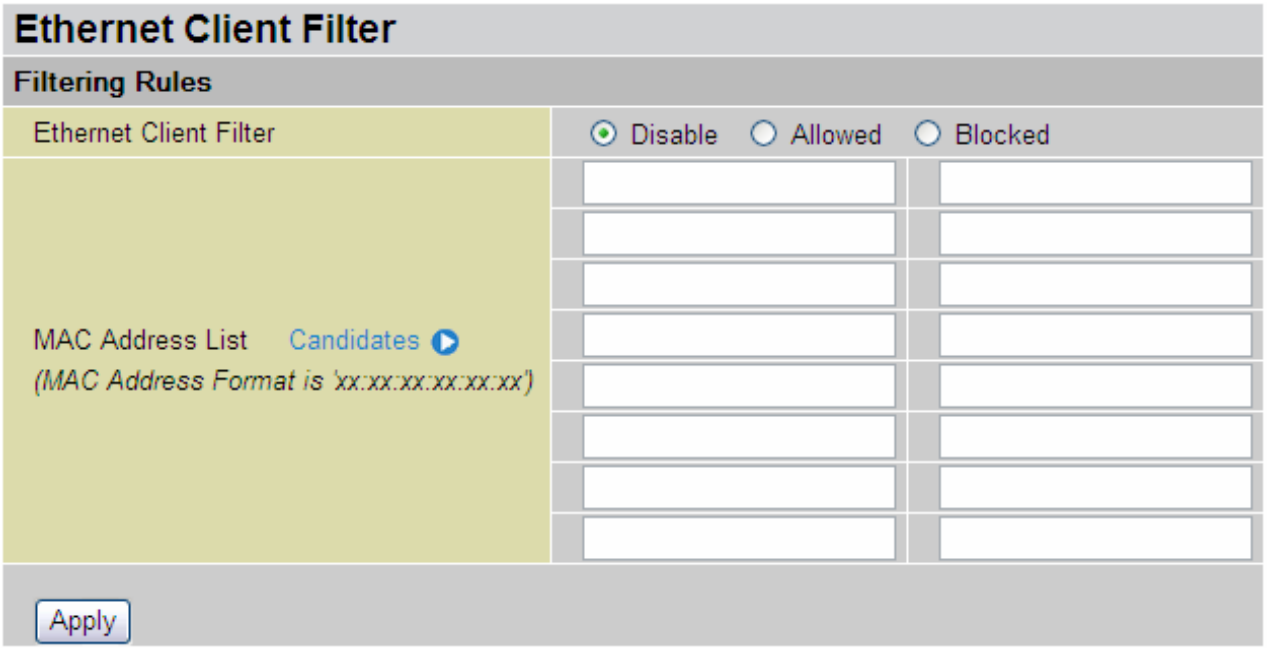
External: There is no NAT on this IP interface and it is connected to the Internet directly. This can be used when your ISP provides multiple public IP addresses.

DMZ: Specify this network as a DMZ area. There is no NAT on this interface.

Ethernet Client Filter

The Ethernet Client Filter supports up to 16 Ethernet network machines and helps you to manage your network control, accepting traffic from specific authorized machines or restricting unwanted machine(s) from access your LAN.

There are no pre-define Ethernet MAC address filter rules; you can add the filter rules that meet your requirements.



Ethernet Client Filter: Default setting is **Disable**.

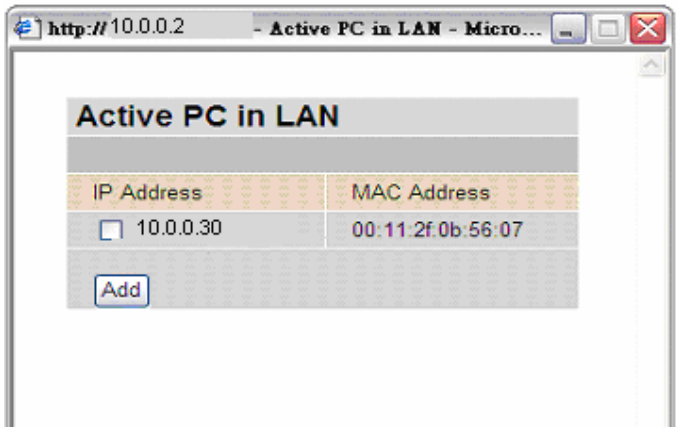
- **Allowed:** check to authorize a specific device to access your LAN by insert the MAC Address in the space provided or click Candidates. Make sure your PC's MAC is listed.
- **Blocked:** To prevent unwanted device accessing your LAN, insert the MAC Address in the space provided or click Candidates. Make sure your PC's MAC is not listed.

The maximum number of clients is 16. The MAC addresses are 6 bytes long; they should be presented only in hexadecimal characters. The number **0** - **9** and letters **a** - **f** are acceptable.

Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.

Candidates: automatically detects devices connected to the router through the Ethernet. .

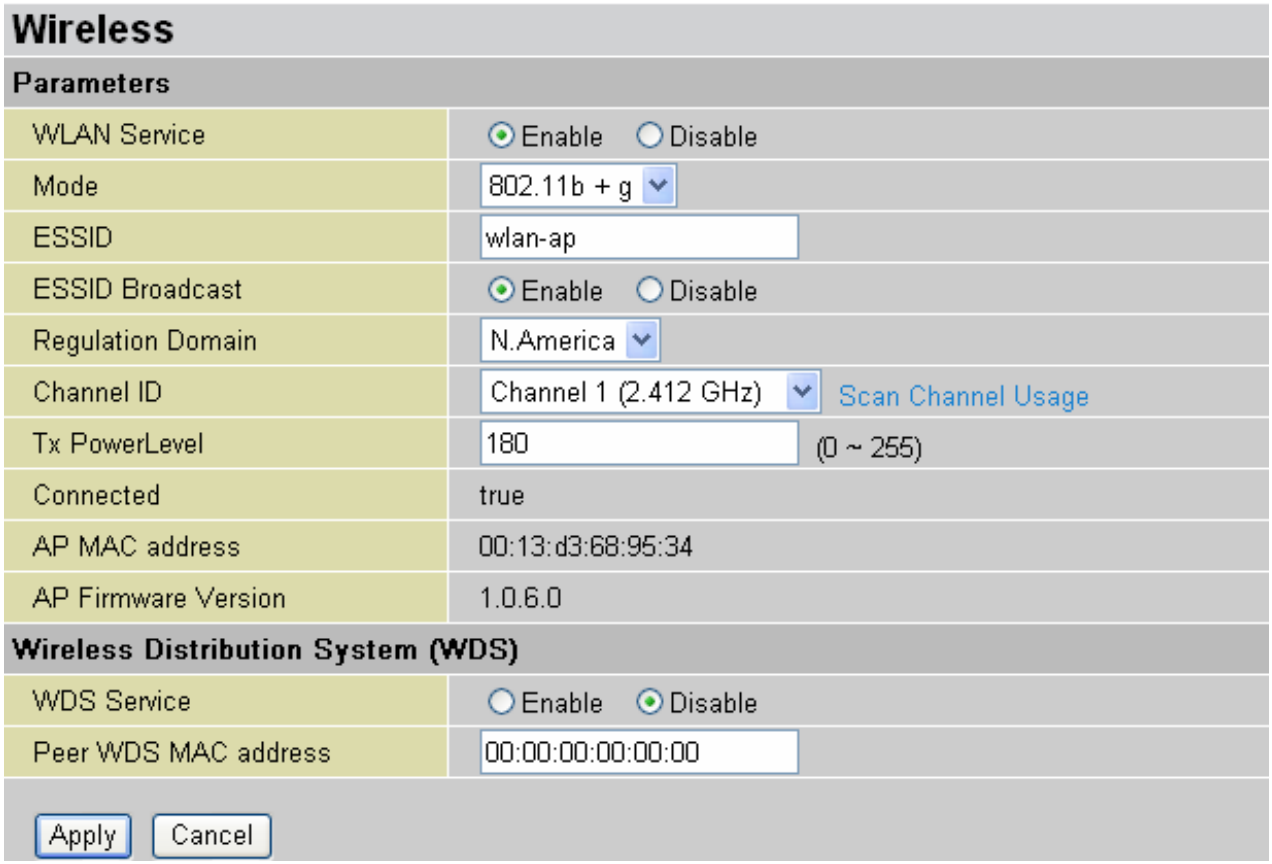
Candidates → **Active PC in LAN**



Active PC in LAN displays a list of individual Ethernet device's IP Address & MAC Address which are connected to the router.

You can easily allow or block a computer by checking the box next to the IP address. Then click **Add** to insert to the Ethernet Client Filter table. The maximum number of Ethernet clients is 16.

Wireless



Parameters

WLAN Service: Default setting is **Enable**. If you do not have any wireless devises (802.11g or 802.11b) on your network, select **Disable.**

Mode: The default setting is **802.11b+g** (Mixed mode). If you do not know what type of wireless devises you have, or have both 11g and 11b devices on your network, then keep the default setting (**mixed mode)**. From the drop-down menu, you can select **802.11g** if you have only 11g clients on your network or if you have only 11b clients on your network, then select **802.11b**.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish it from other AP's. For security purposes, change the default AP ID (**wlan-ap)** to a unique ID name. The ESSID is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the same ESSID as the AP so that you will be able to connect to it .
Note: It is case sensitive and must not excess 32 characters.

ESSID Broadcast: ESSID Broadcast is the function that controls the Routes transmission of its ESSID. This transmission enables wireless clients to detect the presence of the AP when they search for AP;s to connect to. The default setting is **Enabled.**

- **Disable: If** you do not want broadcast your ESSID. Any client using "any" wireless setting cannot discover the Access Point (AP) of your router.
- **Enable:** Any client using the "any" setting can discover the Access Point (AP).

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection ID channel that you would like to use. Use the *Scan Channel Usage* to help to select non-occupied wireless channel.

- **Scan Channel Usage:** Wireless channel scan takes up to 14 seconds to survey the wireless channels In the surrounding area. The result will show which of the wireless channels are already

being used , and wich are available for use.

Note: Wireless performance will be degraded if you select a channel that is already being occupied by other AP(s).

TX PowerLevel: **This** function enhances the wireless transmitting signal strength. Users may adjust this power level from minimum 0 up to maximum 255.

Note: Maximum power Level is not necessarily the best choice in all cases. choose the most suitable level for your network and environment.

Connected: Shown as **true** or **false**. This is the connection status between the wireless card and the network.

AP MAC Address: this is the unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

Wireless Distribution System (WDS)

This is a wireless access point mode that enables wireless linking and communication with other access points. It is easy to install - simply define the peer AP's MAC address. The WDS system gives a cost saving and flexible method of extending wireless range, since no extra wireless client device is required to bridge between two access points. Using WDS, the user can extend an existing wired or wireless infrastructure network to create a larger network.

In addition, the WDS connection can provide network security in WEP mode. The WEP key encryption must be the same for both access points.

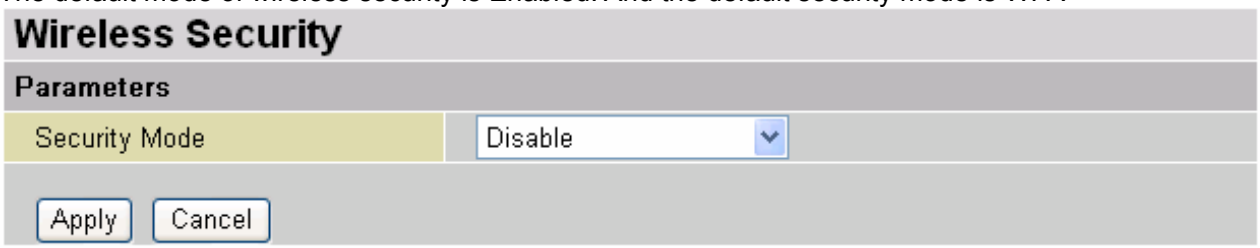
WDS Service: The default setting is **Disabled.** Check **Enable** radio button to activate this function.

Peer WDS MAC Address: this is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to allow the AP's to acknowledge and communicate with each other.

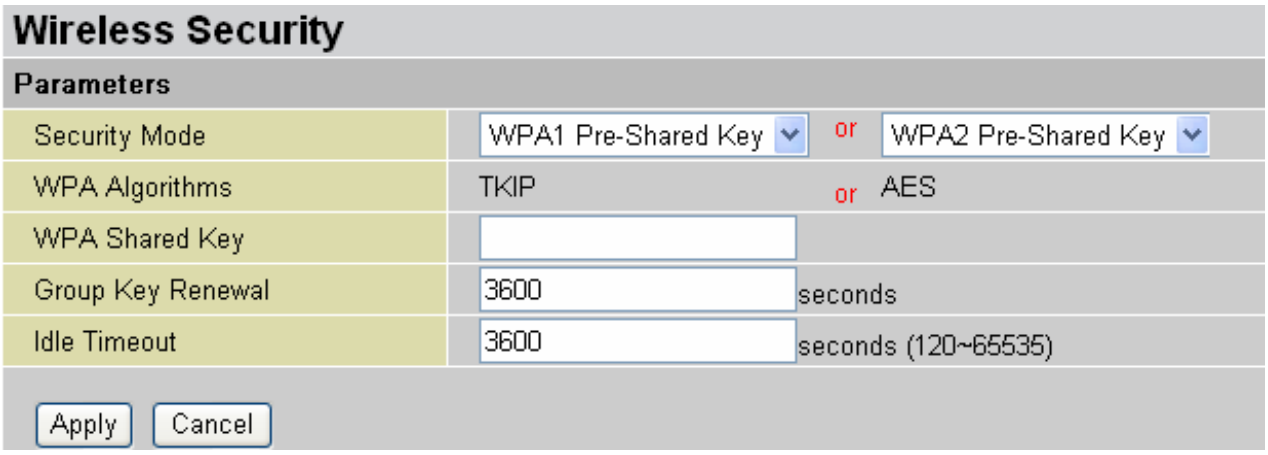
Note: For MAC Address, Semicolon (:) must be included.

Wireless Security

You can disable or enable WPA or WEP for protecting your wireless network.
The default mode of wireless security is Enabled. And the default security mode is WPA



WPA-PSK (TKIP) / WPA-PSK (AES) Pre-Shared Key



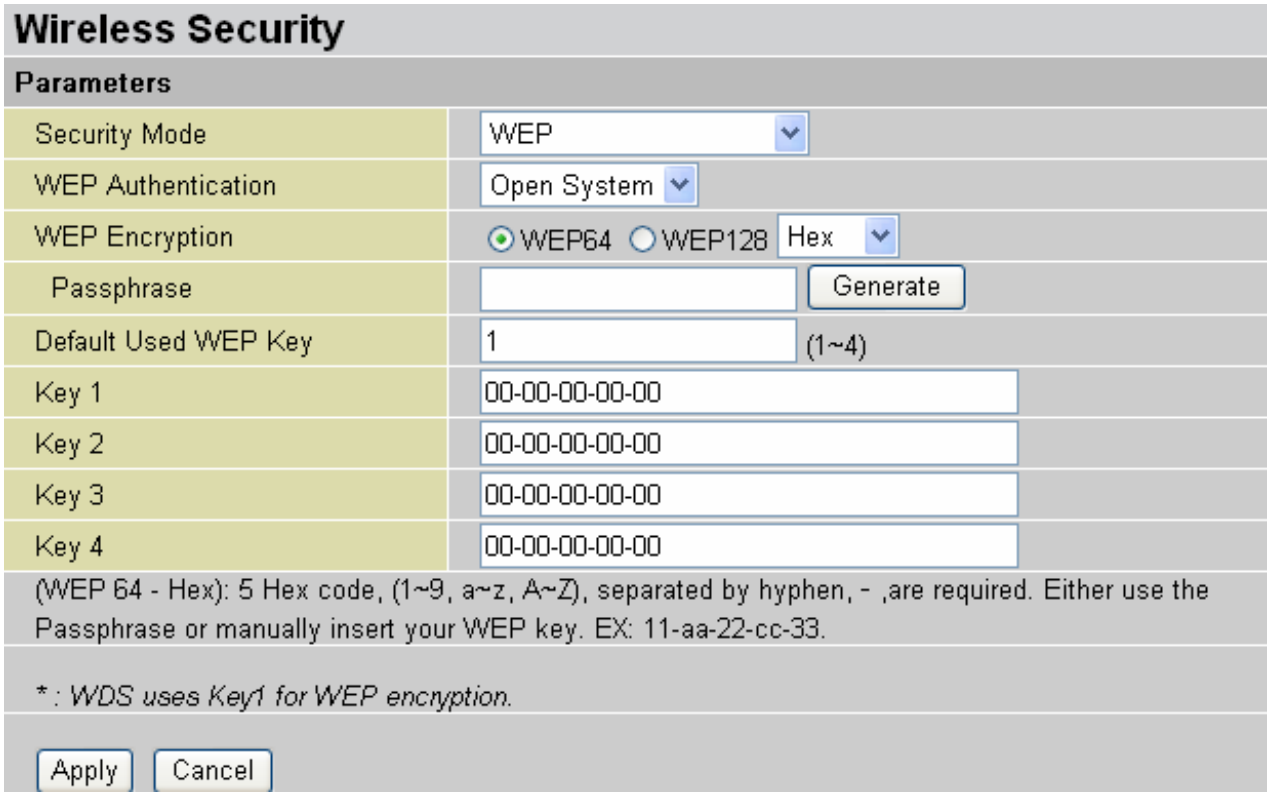
WPA Algorithms: There are two types of WPA-PSK security : WPA1 and WPA2. WPA1 adopts the TKIP (Temporal Key Integrity Protocol) encrypted algorithm, which incorporates Message Integrity Code (MIC), to provide protection against hackers. The WPA2 adopts the CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithm.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters. By default, your Router is provided with a unique Key. This key is also given on a label on the underside of your router/

Group Key Renewal: The time interval for changing the security key automatically between wireless client and Access Point (AP). Default value is **3600** seconds.

Idle Timeout: The default idle timeout is **3600** seconds. The timeout value is for when no data traffic is send or received. If Router detects no traffic on the wireless interface, it will start a timer, and drop the session when the timer reaches the defined timeout value. A new session will be established when further data is sent.

WEP



WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64.

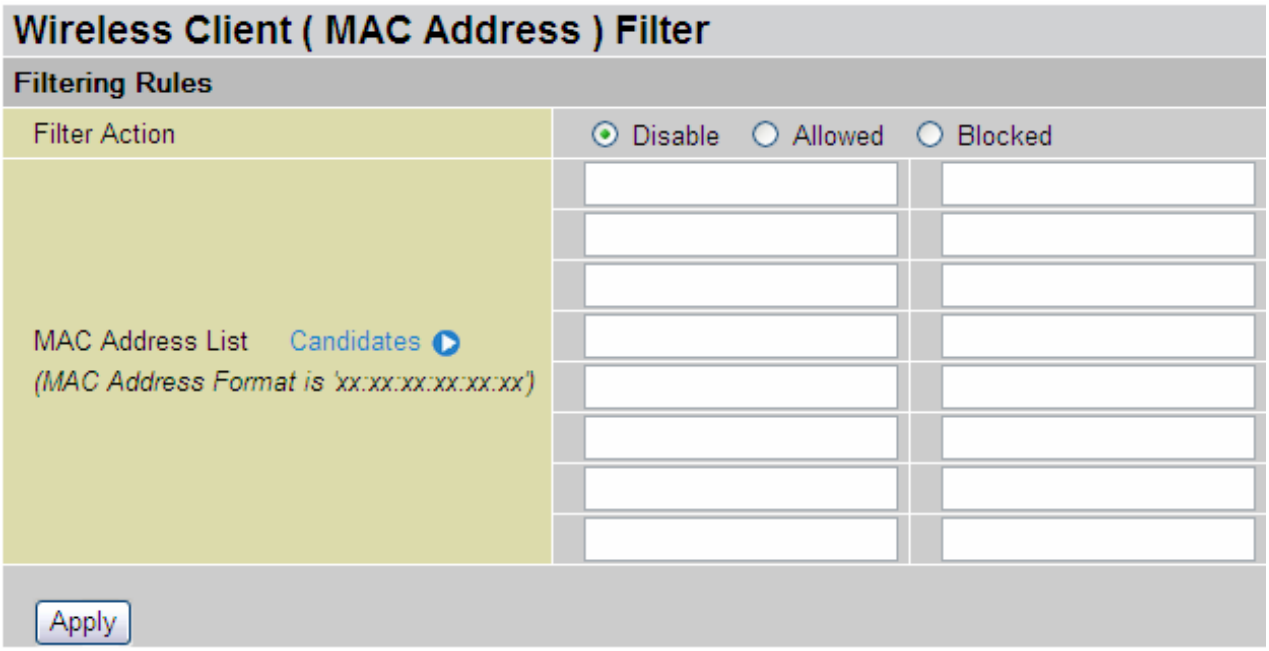
Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. **Default Used WEP Key:** Select the encryption key ID; please refer to **Key (1~4)** below.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-". For example, using WEP64, 11-22-33-44-55 is a valid key, whilst 1122334455 is invalid.

Wireless Client / MAC Address Filter

The MAC Address supports up to 16 wireless network machines and helps you to manage your network control to accept traffic from specific authorized machines or to restrict unwanted machine(s) from accessing your LAN.

There are no pre-define MAC Address filter rules; you can add the filter rules that meet your requirements.



Wireless Client Filter: Default setting is **Disable**.

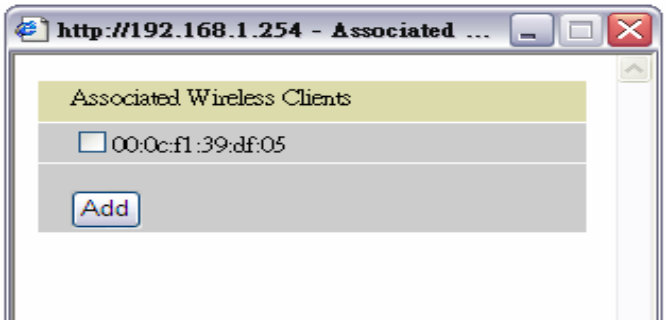
- **Allowed:** To authorize a specific device accessing your LAN, insert the devises MAC Address in the space provided, or click Candidates. Make sure your computer's MAC is listed.
- **Blocked:** To prevent unwanted devices from accessing the LAN, insert the MAC Address of an unwanted computer into the space provided, or click Candidates. Make sure your computer's MAC is not listed.

The maximum number of clients is 16. MAC addresses are 6 bytes long; they are presented only in hexadecimal format. The number **0** - **9** and letters **a** - **f** are acceptable. MAC addresses are 6 bytes long

Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.

Candidates: **T**his function automatically detects devices connected to the router through the Wireless AP . .

Candidates →**Associated Wireless Clients**



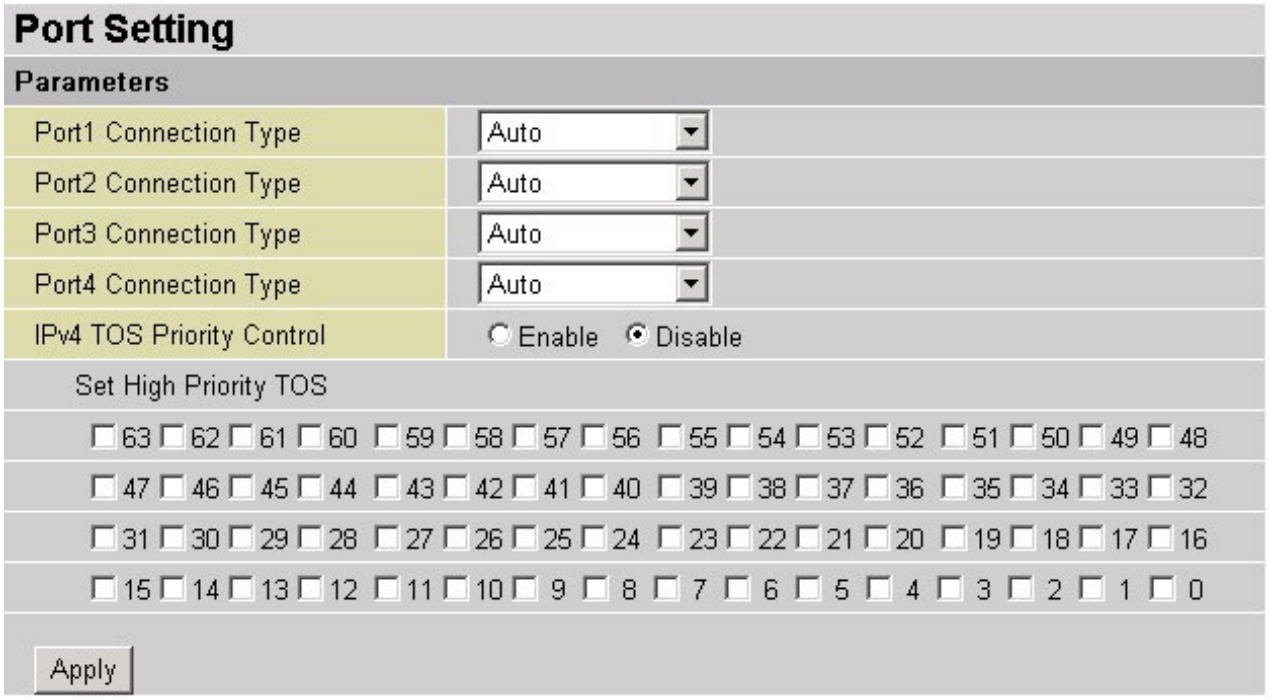
Associate Wireless Client displays a list of individual wireless device's MAC Address that are currently connected to the router.

You can easily add a particular client to the Allow or Block list by checking the box next to the MAC

address and selecting **Add** to insert to the client into the Wireless Client (MAC Address) Filter table.

Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well as allowing users to tweak the performance of their network.


Port Setting
Parameters
Port1 Connection Type
Auto
Port2 Connection Type
Auto
Port3 Connection Type
Auto
Port4 Connection Type
Auto
IPv4 TOS Priority Control
Enable
Disable
Set High Priority TOS
63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48
47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Apply

Port # Connection Type: this is where you can customize the connection type of each of the routers Ethernet ports. There are Six options to choose from: Auto, disable, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure a particular Ethernet port to one of the different types to solve compatibility issues. The default is **Auto**, which users should keep unless there are specific problems with computers not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

This feature uses bits 0-5 to classify the packet's priority. If the packet is high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the TOS field matches the checked values in the table (0 to 63), this packet will be treated as high priority.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to computers on your network if they are configured to obtain IP addresses automatically.

DHCP Server

Configuration	
DHCP Server Mode	○ Disable
	◉ DHCP Server
	○ DHCP Relay Agent
Next	

DHCP Server Status	
Allow Bootp	true
Allow Unknown Clients	true
Enable	true
Subnet Definitions	
Subnet Value	192.168.1.0
SubNetmask	255.255.255.0
Maximum Lease Time	86400 seconds
Default Lease Time	43200 seconds
Use local host address as DNS server	true
Use local host address as default gateway	true
Get subnet from IP interface	iplan
IP Range *192.168.1.100- 192.168.1.199*	
Option *domain-name-servers= 0.0.0.0*	

To disable the router's DHCP Server, check **Disabled** and click **Next,** then click **Apply.** When the DHCP Server is disabled you will need to manually assign a fixed IP address to each Computer on your network, and set the default gateway for each computer to the IP address of the router (by default this is 10.0.0.2).

To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to Computers on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in your LAN (your Local Area Network).

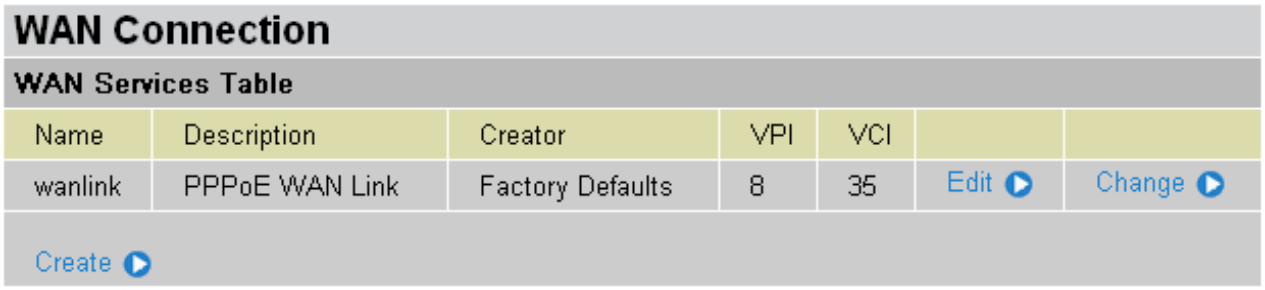
If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client on your LAN. Use this function only if advised to do so by your network administrator or ISP.

Click **Apply** to enable this function.

WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and the Internet. Here are the items within the **WAN** section: **ISP**, **DNS** and **ADSL**.

ISP



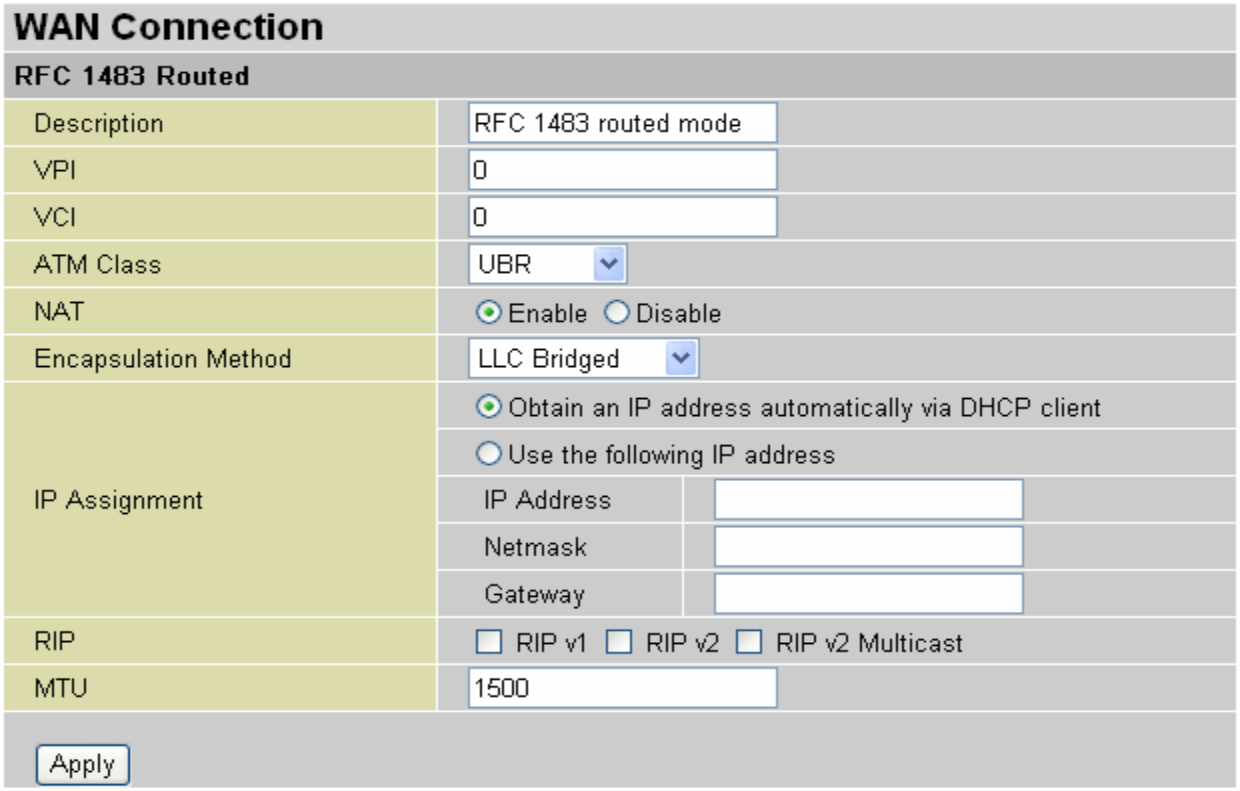
The factory default is PPPoE. Telkom uses this access protocol. If you wish to change any of these parameters, click **Edit**. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

Some ISP may provide more services via different WAN connections. In this case, you can create more than 1 connection by clicking **Create**. The device can support maximum up to 8 WAN connections.

Note: The application of multiple WAN connections is depend on your Service Provider.

A simpler alternative is to select **Quick Start** from the main menu on the left. Please see the Quick Start section of the manual for more information.

RFC 1483 Routed Connections



Description: User-definable name for the connection.

VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Encapsulation method: Selects the encapsulation format, the default is LLC Bridged. Select the option provided by your ISP.

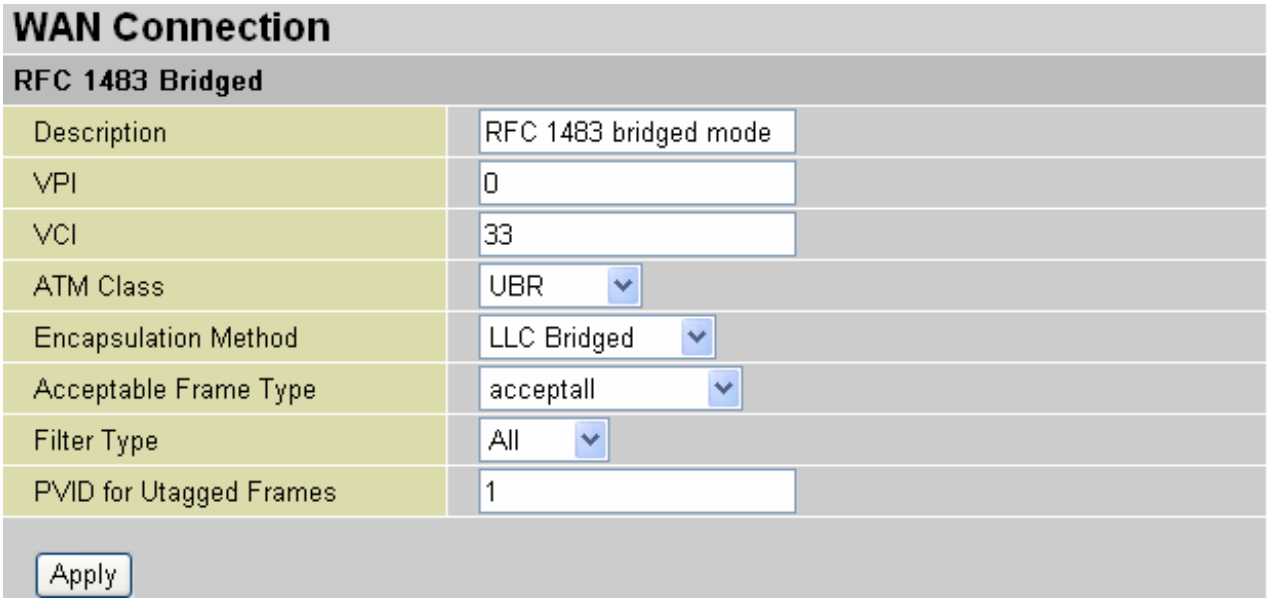
IP Assignment

- **Obtain an IP address automatically via DHCP client:** specify if the Router can get an IP address from the ISP (Internet Service Provider) automatically.
- **Use the following IP Address:** Specify the IP address manually; the IP should be given to you by your ISP.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RFC 1483 Bridged Connections



Description: User-definable name for the connection.

VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

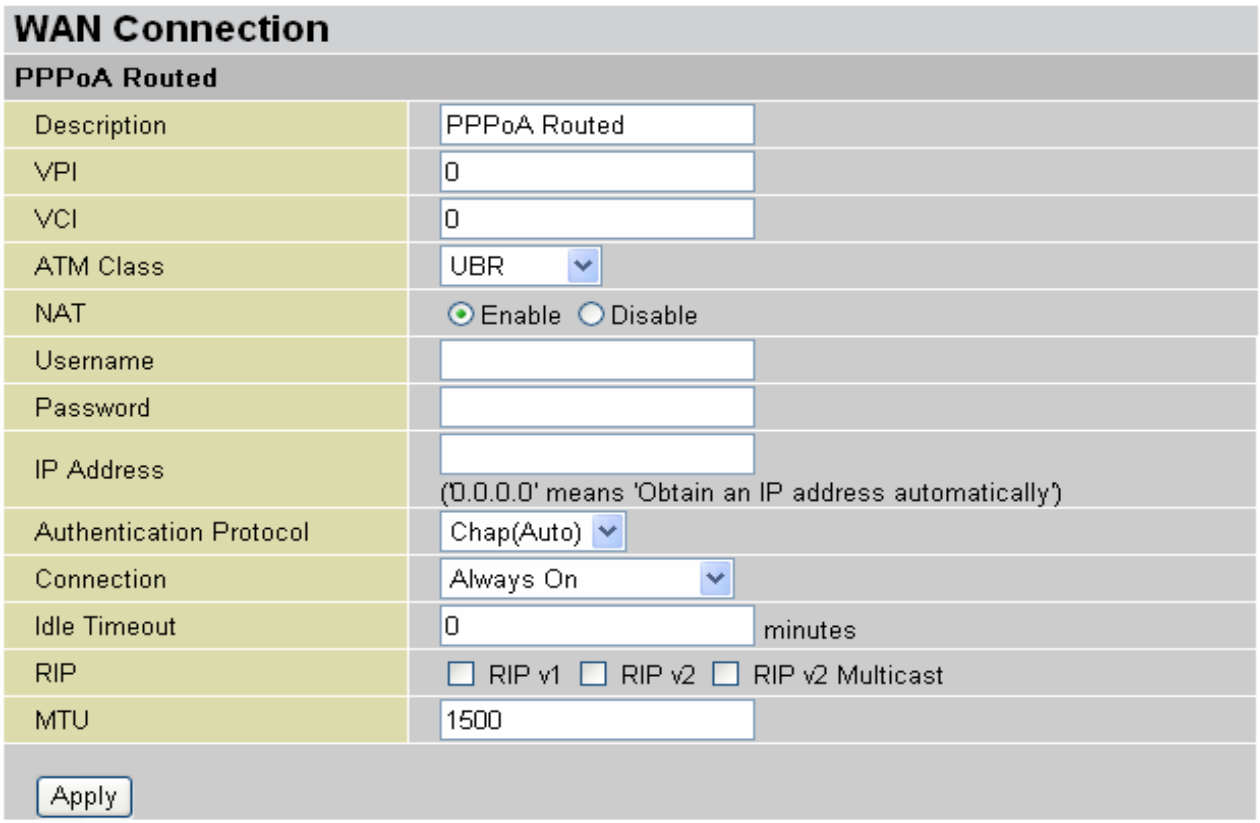
Acceptable Frame Type: Specify what kind of traffic can through this connection, all traffic or only VLAN tagged traffic.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

PVID for Untagged Frames: PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID. The valid value range for PVID is 1~4094.

PPPoA Routed Connections



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

IP Address: Specify IP addresses that are allowed to logon and access the router's web server..

Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon to the device and modify data.

Authentication Protocol Type: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

- **Always on:** If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
- **Connect on Demand:** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

⊙ **Detail:** You can define destination port and packet type (TCP/UDP) information that will not result in the router checking the timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoA)

LLC Header: Selects encapsulation mode, select true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: This setting specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: This sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: This sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: This controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

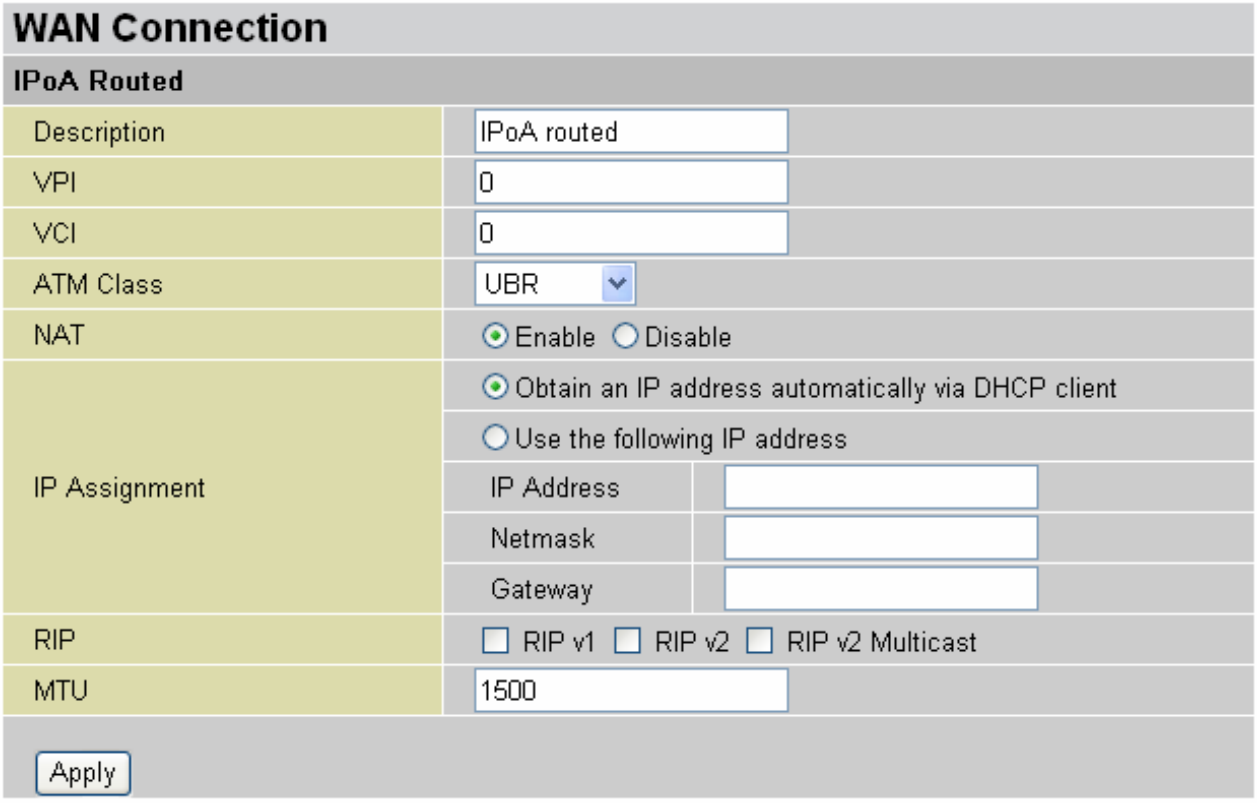
Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: This specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

IPoA Routed Connections



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

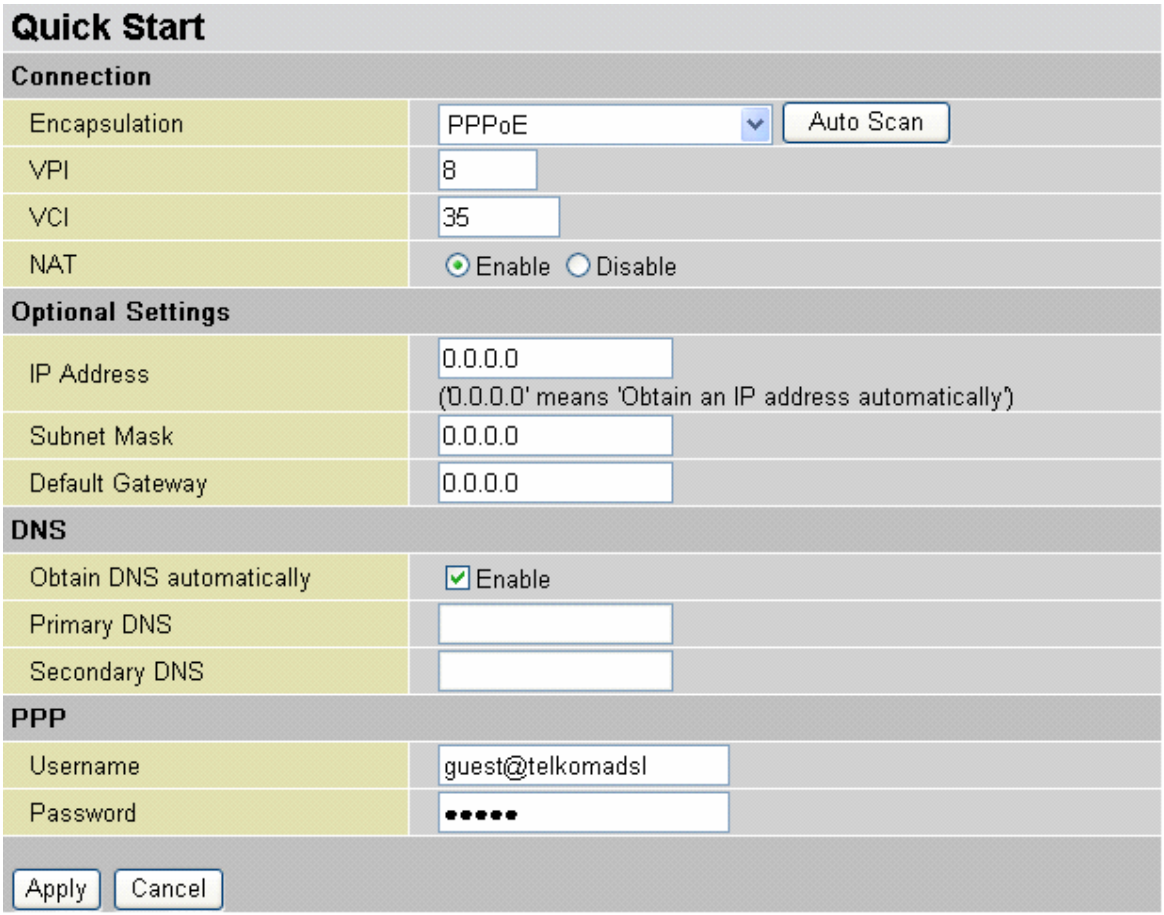
IP Assignment

- **Obtain an IP address automatically via DHCP client: This** specifies if the router is to get an IP address from the ISP (Internet Service Provider) automatically.
- **Use the following IP Address:** this is to specify the IP address manually; this IP should be given by your ISP.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE Connections



Description: User-definable name for this connection.

VPI/VCI: Enter the information provided by your ISP. The Telkom standard settings are 8 and 35.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: This specifies if the router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click **Obtain an IP address automatically via DHCP** (default setting) client to enable the DHCP client function or click **Specify an IP address** to disable the DHCP client function, and specify the IP address manually. To connect to the Telkom network, please leave this at the default value .

Authentication Protocol: Default is Chap(Auto). Your ISP will advise you whether to use Chap or Pap.

Connection

- **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

- **Connect on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined period of time.

- **Detail:** You can define destination port and packet type (TCP/UDP) information that will not result in the router checking the timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer..

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoE)

LLC Header: Selects encapsulation mode. Select true to use LLC or false to use VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: This specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: This sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: This sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: This controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: This controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

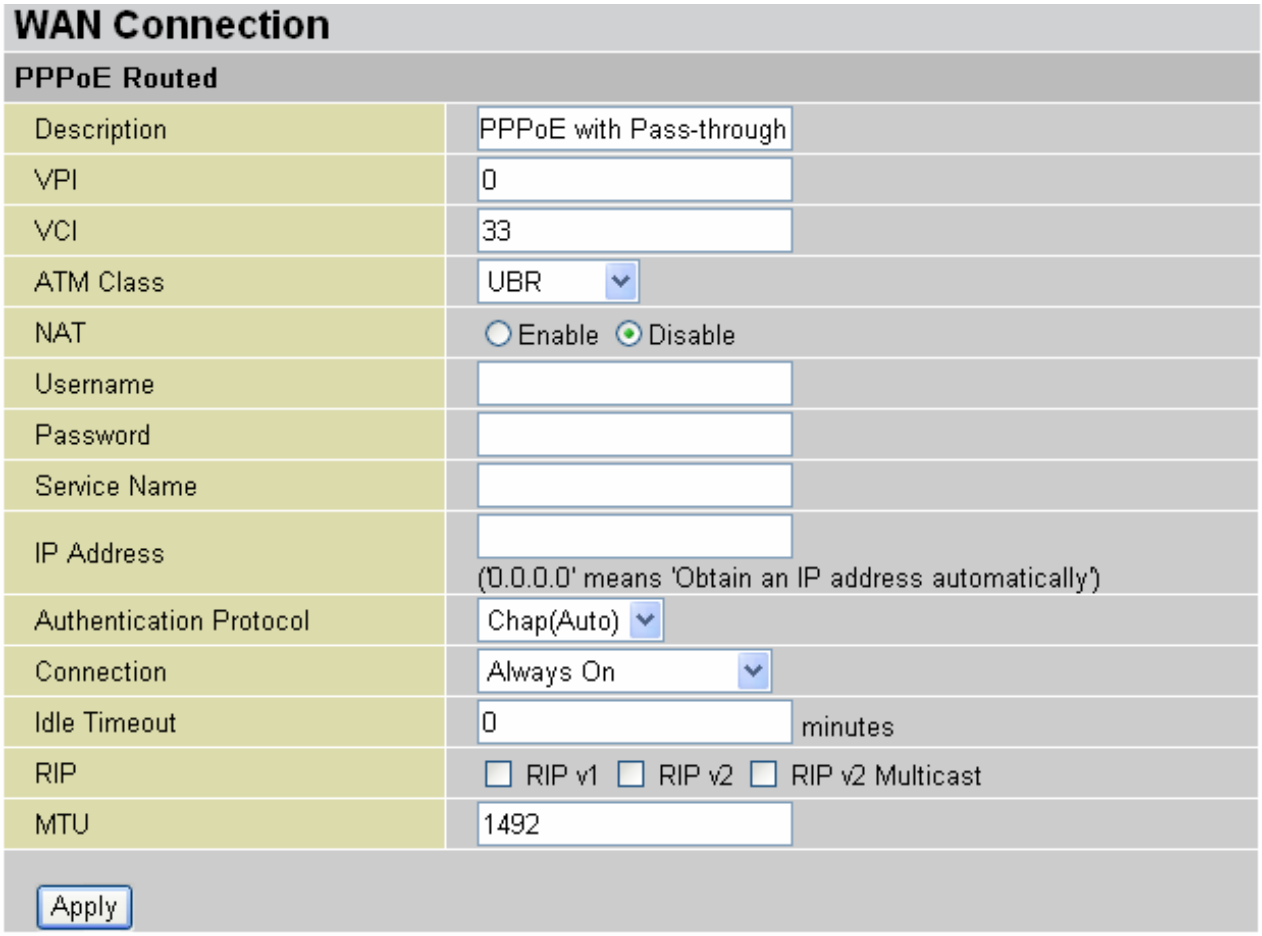
Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

PPPoE with Pass-through Connections

PPPoE with pass-through adopts the following method: PPPoE Routed mode + 1483 Bridge Mode. With pure PPPoE connection, the router can get one WAN address for the router. With the PPPoE and PPPoE pass-through, concurrently, it allows users to have a WAN address assigned to the router but also able to get another WAN IP from their ISP using PPPoE dialer (e.g WinPoETor Windows XP PPPoE Dialer) at the same time.



Description: User-definable name for this connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: This specifies if the router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click **Obtain an IP address automatically via DHCP** client to enable the DHCP client functionality or click **Specify an IP address** to disable the DHCP client functionality, and specify the IP address manually. The setting of this item is specified by your ISP.

Authentication Protocol: Default is Chap(Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

- **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- **Connect on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

- **Detail:** You can define destination port and packet type (TCP/UDP) information that will not result in the router checking the timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.
- **RIP:** RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Advanced Options (PPPoE)

LLC Header: Selects encapsulation mode. Select true to use LLC or false to use VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: This specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: This sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: This sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: This controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: This controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

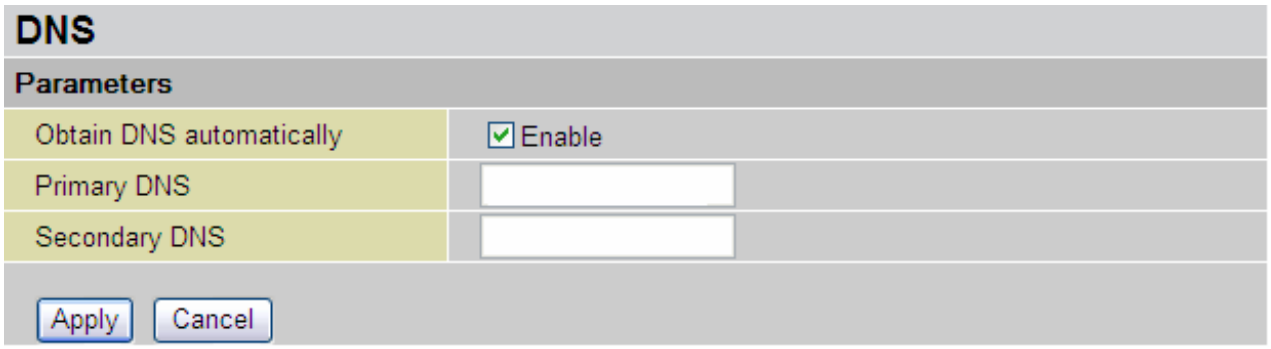
Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

DNS



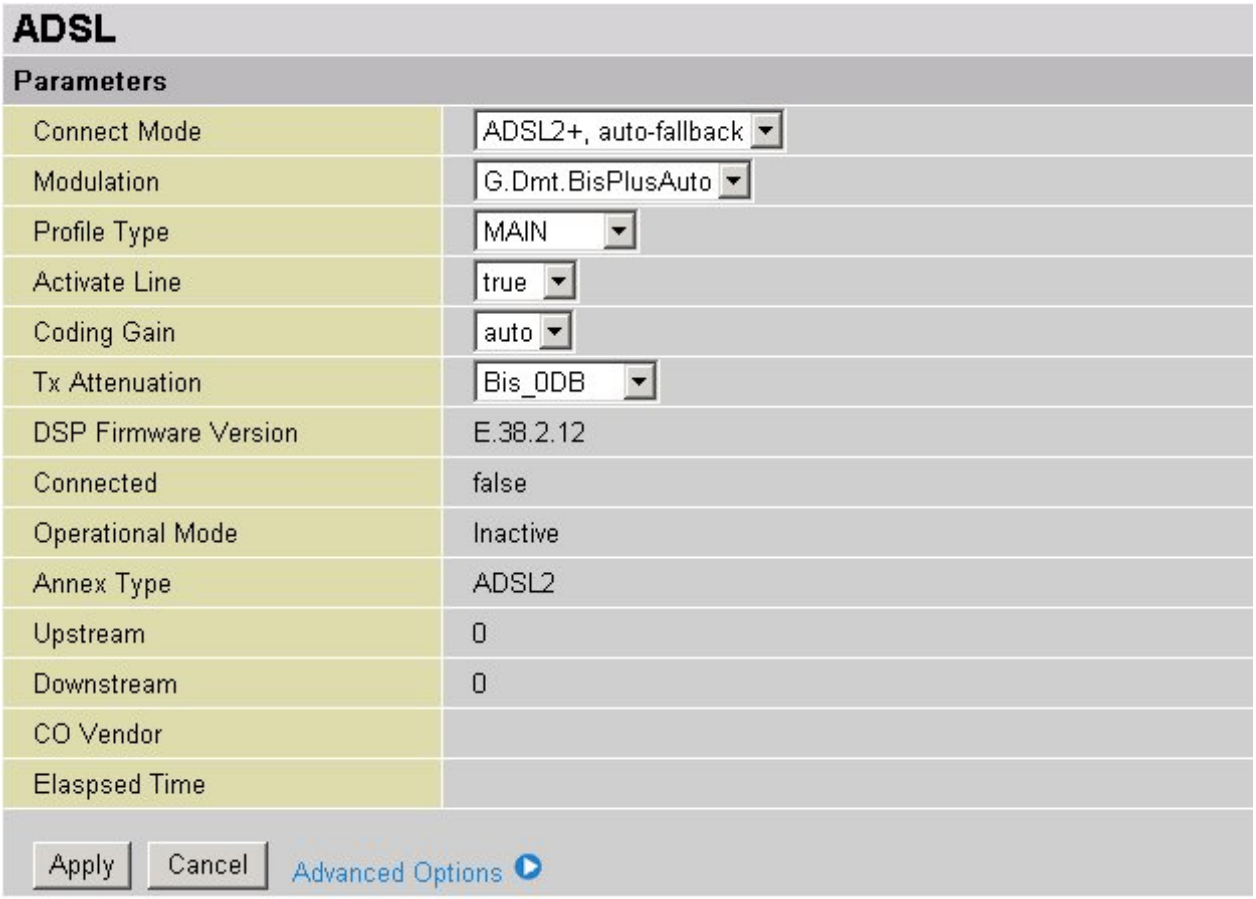
A Domain Name System (DNS) contains a mapping table for mapping between Domain Names and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com as well as an IP address. An IP address is a 32-bit number in the form of *xxx.xxx.xxx.xxx*, for example 10.0.0.2. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides it when you logon. To use this automatically supplied DNS check the **Enable** box. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave the configuration field blank.

Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address manually.

If you choose one of the other three protocols ─ RFC1483 Routed/Bridged or IPoA, please check with your ISP as it may provide you with an IP address for their DNS server. You will need to enter the DNS IP address if you set the DNS of your PC to the LAN IP address of this router.

ADSL



Connect Mode: This mode will automatically detect your ADSL line mode, ADSL2+, ADSL2, G.dmt, G.lite, T1.413, AnnexM2 or AnnexM2+. But in some areas, multimode cannot detect the ADSL line mode very well. If it is the case, please adjust the ADSL line code to G.dmt first. If it still fails, ,please check with your ISP for line connect information.

Activate Line: Select **false** and then select **true** to activate any new **Connect Mode** settings.

Coding Gain: This reduces the router's transmit power and will effect to router's downstream performance. General, the higher the gain, the higher the downstream rate, but sometimes a gain that is too high will cause an unstable ADSL connection. The configurable ADSL coding gain is from 0 dB to 7dB, or automatic.

Tx Attenuation: **This is** the ADSL transmission power that the modem is using. The lower the power the better performance in router's upstream. Configurable value is between 0~12.

DSP Firmware Version: Current ADSL line code firmware version.

Connected: Display current ADSL line sync status.

Operational Mode: Display current ADSL mode standard (Operational Mode) that your Router is using when ADSL line has sync.

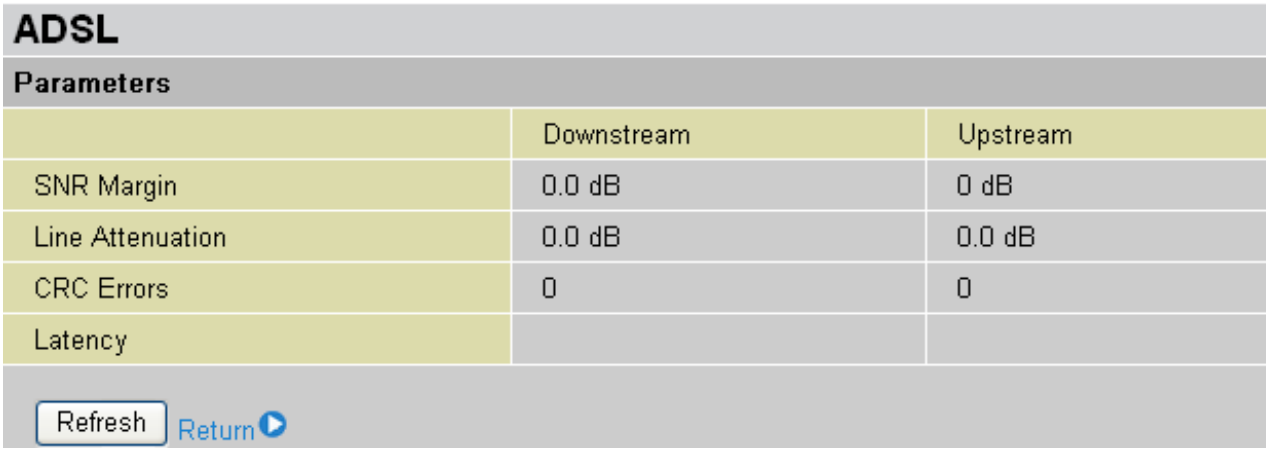
Annex Type: ADSL Annex A, which works over a standard telephone line. Annex B, which works over an ISDN line. In South Africa, we always use Annex A

Upstream: Display current upstream rate of your ADSL line.

Downstream: Display current downstream rate of your ADSL line.

Advanced Options

ADSL Parameters help to interpret your ADSL line statistics.

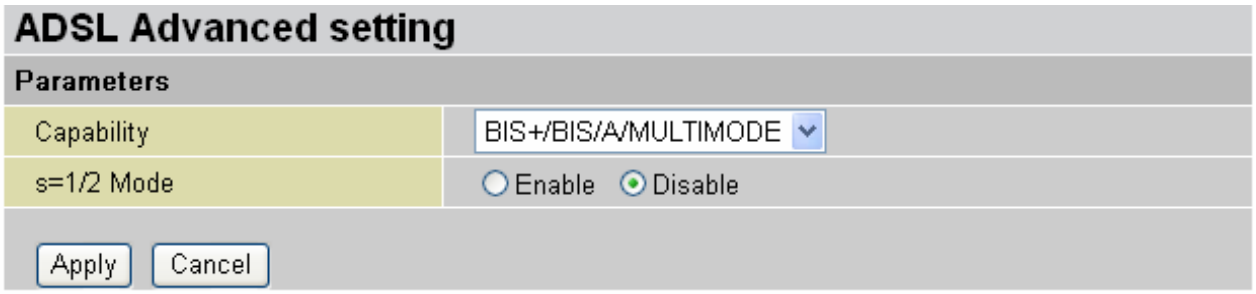


SNR Margin: This is known as Signal to Noise Ration Margin. It is the ratio between DSL strength and signal noise. This margin is measured in decibels (dB). Higher the dB figures better the DSL strength is relative to the noise, and better chance to get faster speed. THE HIGHER THE BETTER

Line Attenuation: This measures the signal loss in decibel (dB) between the DSLAM and the router. The lower the attenuation dB figures, the better the DSL strength/speed. THE LOWER THE BETTER.

CRC Errors: It is known as Cyclic Redundancy Check Error. It is the use of checksums to detect transmission errors.

Latency: This includes two channels, Fast and Interleaved. It displays the channel adopted by your ISP.



Capability: There are more combinational ADSL modulation modes to be selected.

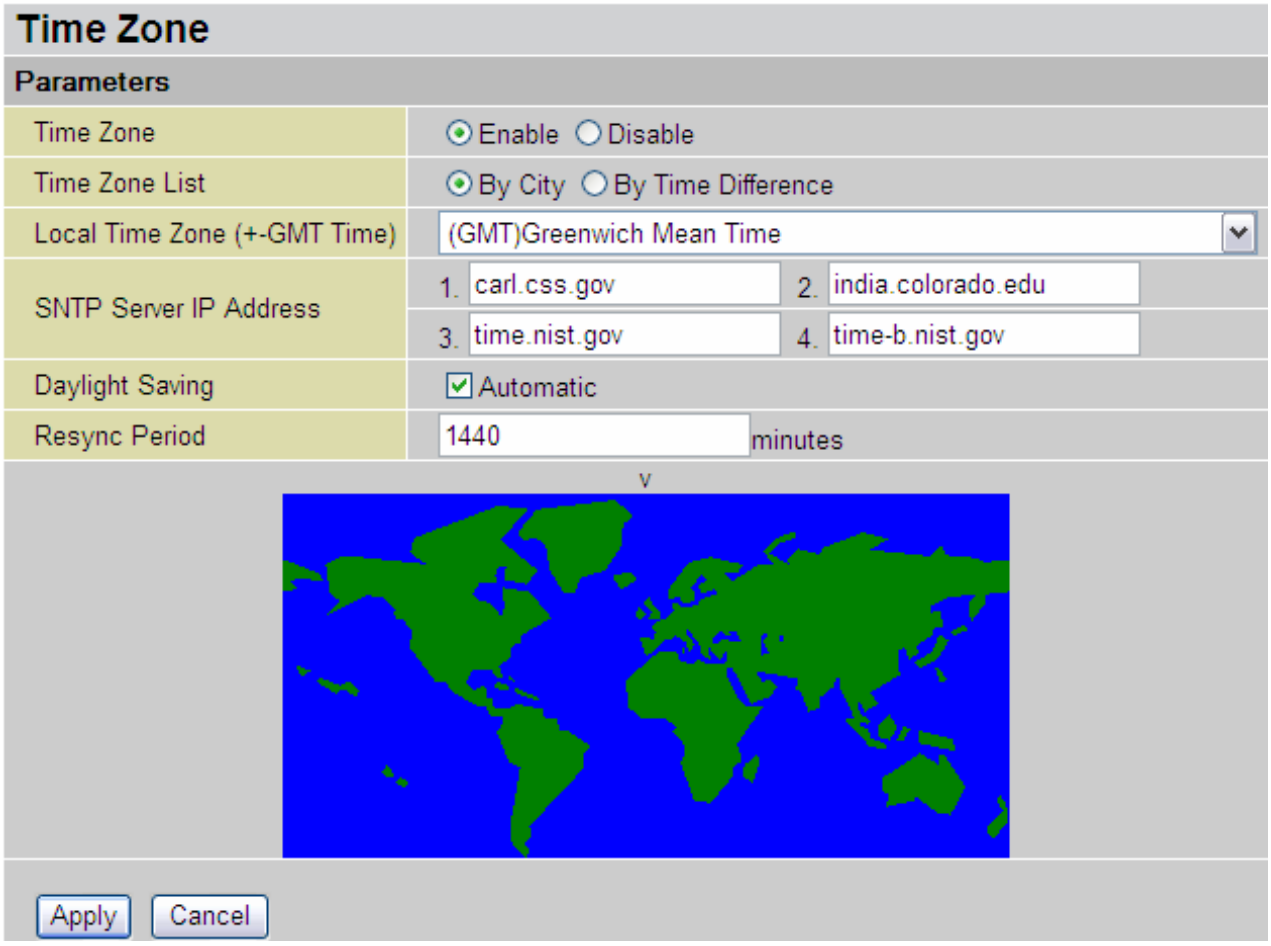
- **GDMT:** ADSL connection will be limited to ADSL1 (G.DMT / G.Lite) only.
- **BIS+:** ADSL connection will be limited to ADSL2+ only. (If you are ADSL1 subscriber DO NOT select this option).
- **BIS+/T1413:** ADSL connection will be limited to ADSL2+ and ADSL1 T1.413 only.
- **BIS+/BIS:** ADSL connection will be limited to ADSL2+ and ADSL2 only.
- **BIS+/BIS/GDMT/T1413:** ADSL connection will be limited to ADSL2+, ADSL2 and ADSL1 G.DMT & G.Lite & T1.413.
- **BIS+/BIS/T1413:** ADSL connection will be limited to ADSL2+, ADSL2 and T1.413.
- **BIS+/BIS/GDMT:** ADSL connection will be limited to ADSL2+, ADSL2 and ADS1 (G.DMT/G.Lite) only.
- **DISABLE:** This disable function will disconnect your ADSL synch. Use it with caution.

S=1/2 Mode: This is a ADSL1 protocol that can increase the downstream speed up to 12Mpb. Please check further with your ISP if this option can be enabled or not.

System

Here are the items within the **System** section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart** and **User Management.**

Time Zone

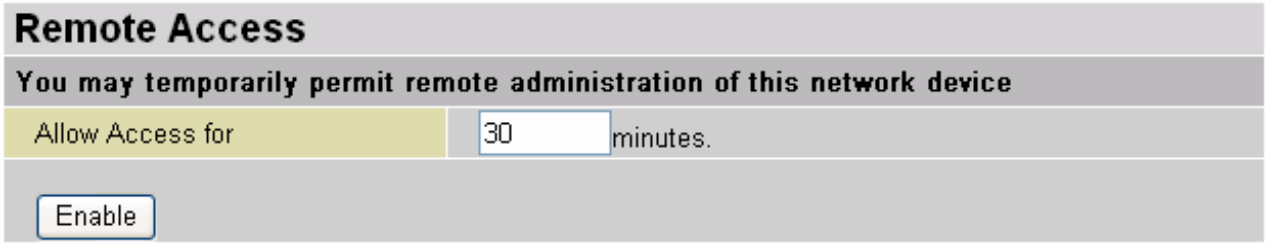


This router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Daylight Saving is also known as ***Summer Time Period.*** Many places in the world adopt this during summer time to move one hour of daylight from morning to the evening in local standard time. Check **Automatic** box to automatically set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

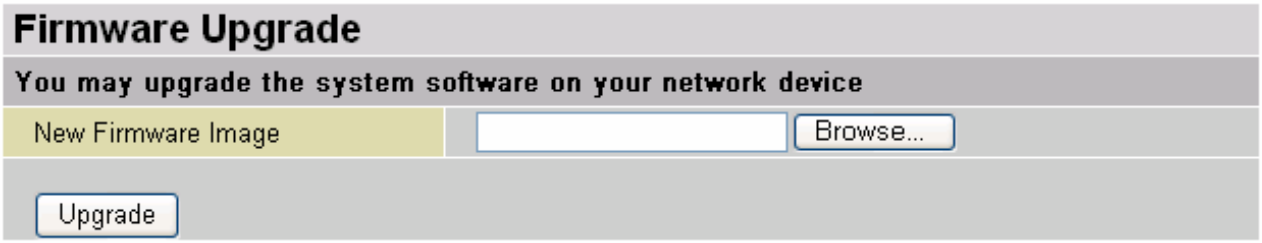
Remote Access



To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router will permit remote access for and click **Enable.** You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

If you wish to permanently enable remote access, choose a time period of **0** minute.

Firmware Upgrade

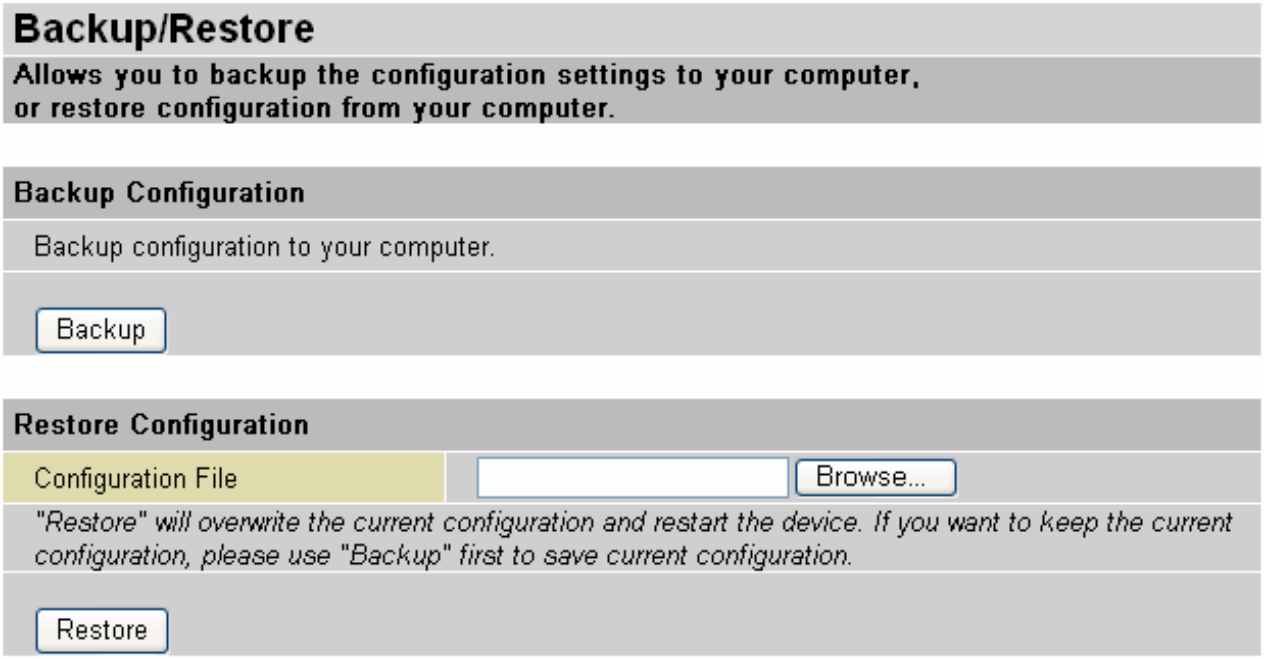


Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore


Backup/Restore
Allows you to backup the configuration settings to your computer,
or restore configuration from your computer.
Backup Configuration
Backup configuration to your computer.
Backup
Restore Configuration
Configuration File
Browse...
"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.
Restore

These functions allow you to save and backup your router's current settings to a file on your Computer, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration, as well as before performing a firmware upgrade.

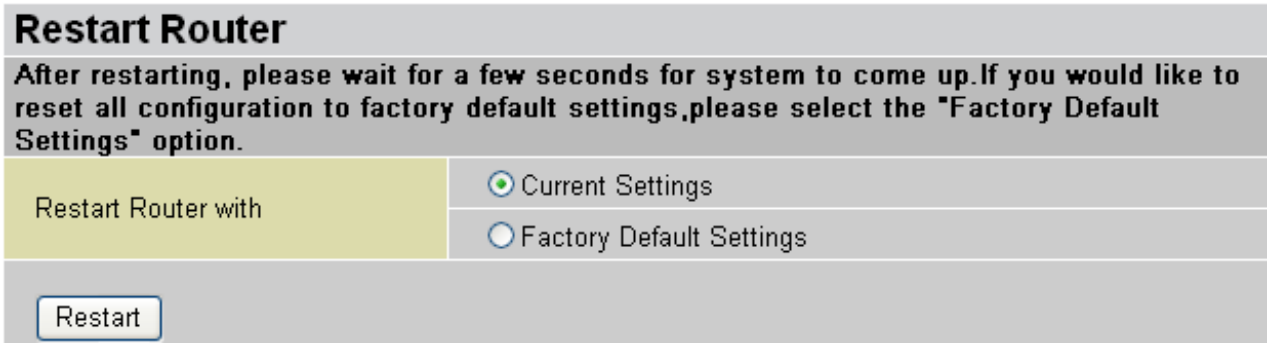
Press **Backup** to select where on your local computer to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your computer to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your computer should not be manually edited in any way.**

After selecting the settings file you wish to use, pressing **Restore** will load those settings into the router.

Restart Router

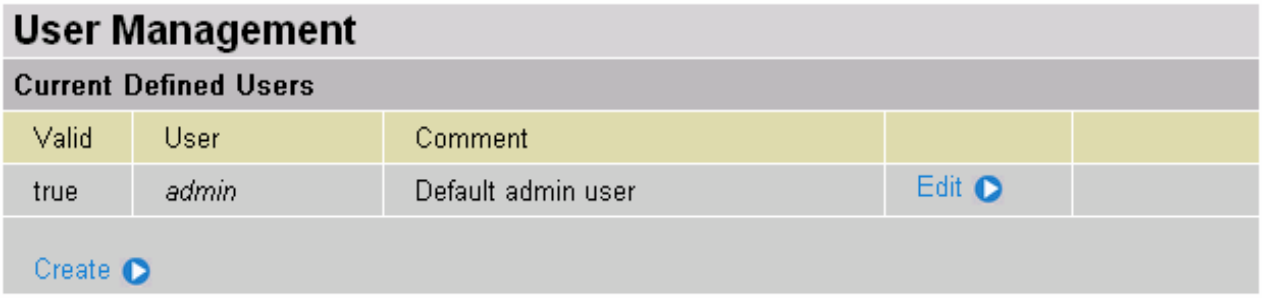
Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).


Restart Router
After restarting, please wait for a few seconds for system to come up.If you would like to reset all configuration to factory default settings,please select the "Factory Default Settings" option.
Restart Router with
Current Settings
Factory Default Settings
Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

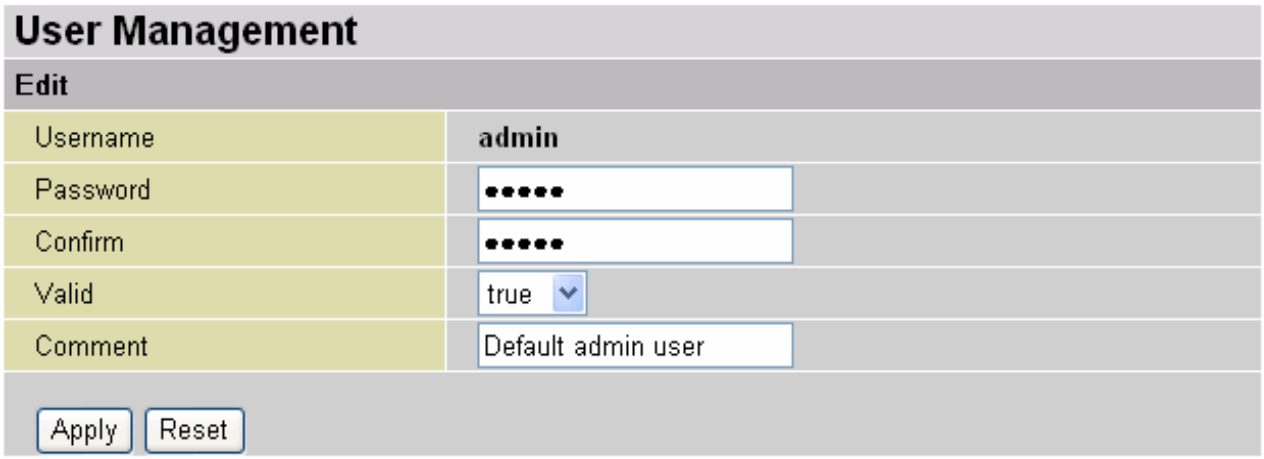
You may also reset your router to factory settings by holding the small RESET pinhole button on the back of your router in for more than 6 seconds whilst the router is turned on, and then power cycling your router.

User Management



In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Create** new users who are able to access the device's configuration interface. Once you have clicked on **Edit,** you are shown the following options:

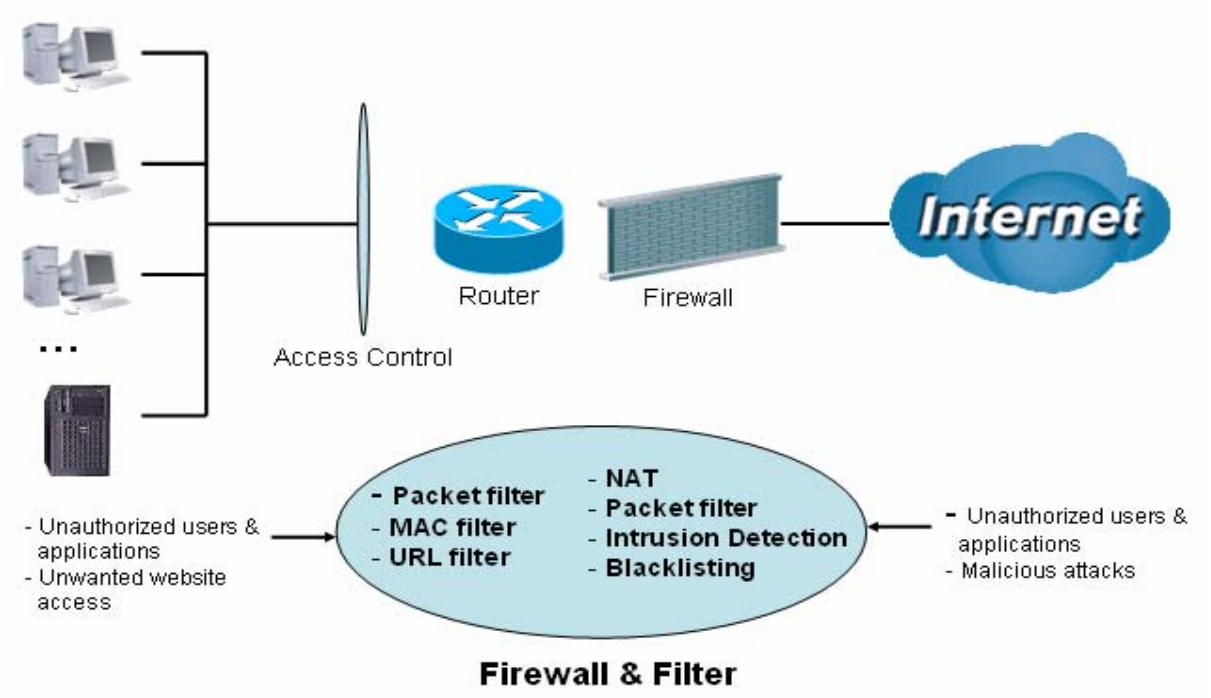


You can change the user's **password**, whether their account is active and **valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however, you can delete any other created accounts by clicking **Delete** when editing the user.

You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT, the router acts as a "natural" Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.



Firewall & Filter

Firewall: Prevents access from outside your network. The router provides three levels of security support:

NAT natural firewall: This masks LAN users' IP addresses making them invisible to outside users on the Internet, thus making it much more difficult for a hacker to target any machine on your network. This natural firewall is on when NAT function is enabled.

When using the Virtual Servers function, your PCs will be exposed to the degree specified in your Virtual Server settings, provided that the ports specified are opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized WAN computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

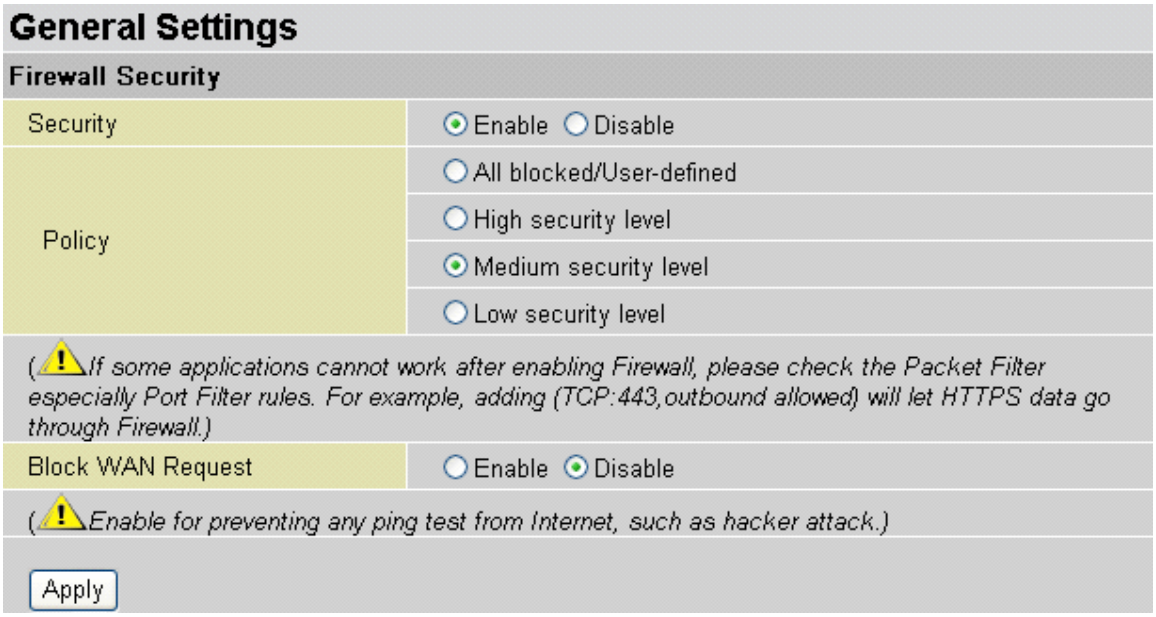
Access Control: Prevents access from computers on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized LAN computers or applications accessing the Internet.

URL Filter: Blocks computers on your local network from unwanted websites.

Here are the items within the **Firewall** section: **General Settings, Packet Filter, Intrusion Detection, URL Filter, IM/P2P Blocking** and **Firewall Log.**

General Settings


General Settings
Firewall Security
Security
Enable
Disable
Policy
All blocked/User-defined
High security level
Medium security level
Low security level
(If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)
Block WAN Request
Enable
Disable
(Enable for preventing any ping test from Internet, such as hacker attack.)
Apply

You can choose not to enable the Firewall and still have access to URL Filter and IM/P2P Blocking, or you can enable the Firewall using preset filter rules and modify the port filter rules as required. The Packet Filter is used to filter packets based-on Applications (Port) or IP addresses.

There are four options when you enable the Firewall, they are:

- **All blocked/User-defined**: No pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.
- **High/Medium/Low security level:** The predefined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

Select either **High, Medium** or **Low security level** to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall functionality is the same for all levels; it is only the list of preset port filters that changes between each setting. For more detailed on level of preset port filter information, refer to **Table 1: Predefined Port Filter**.

If you choose one of the preset security levels and add custom filters, this level of filter rules will be saved and you do not need to re-configure the rules again if you disable or switch to other firewall level.

The "**Block WAN Request**" is a stand-alone function and not related to whether security is enabled or disabled. Mostly this is used to preventing a hacker on the WAN from using any scan tools..

Attempting to perform this action remotely may result in blocking of all access to configuration and managment of the device from the Internet. Use this with caution when connecting over the WAN

Packet Filter

This function is only available when the firewall function is enabled and one of these four security levels is chosen (All blocked, High, Medium and Low). The preset port filter rules in the Packet Filter must be modified according to the level of Firewall which is selected. See **Table1: Predefined Port Filter** for more detail information.

Packet Filter

Add TCP/UDP Filter | Add Raw IP Filter

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
lei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
lei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
lei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
lei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
lei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete
lei_smtp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Block Allow	Edit	Delete
lei_pop3	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Block Allow	Edit	Delete

Example: Predefined Port Filters Rules

The predefined port filter rules for High, Medium and Low security levels are listed. See Table 1.

Note: Firewall – For **Blocked/User-defined**, you must define and create the port filter rules yourself. No predefined rules are configured for these modes.

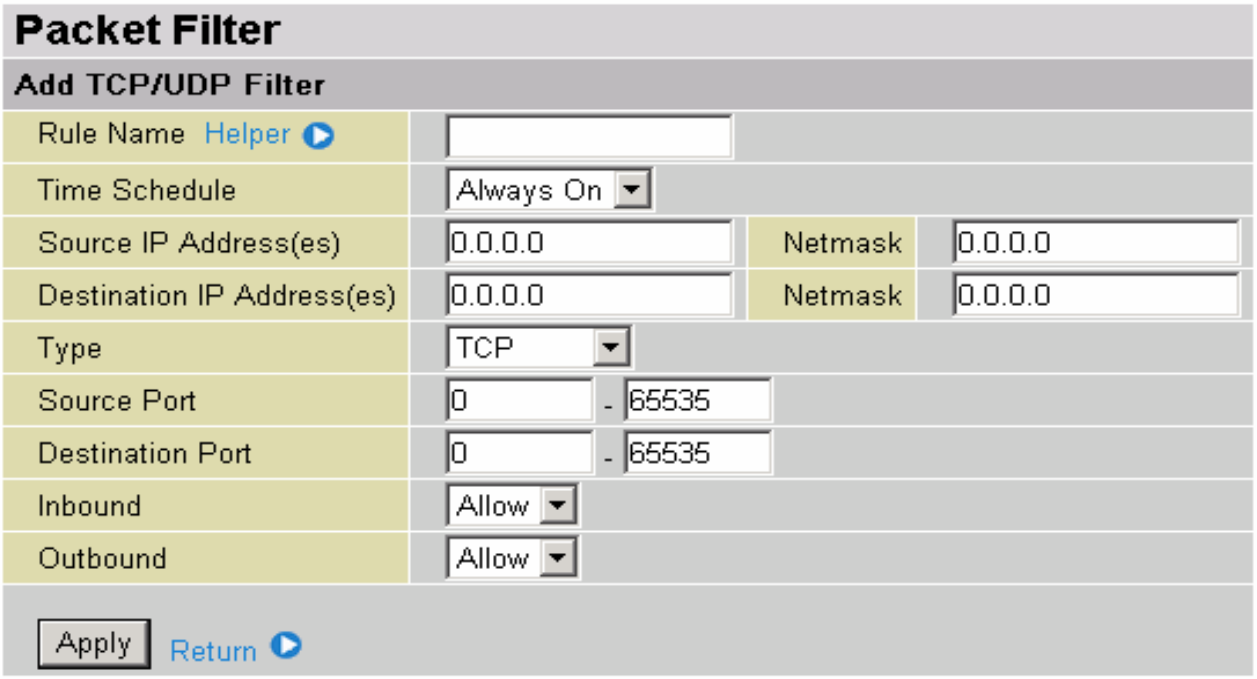
Table 1: Predefined Port Filter

Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP /SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy (8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A

MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN ; **Outbound:** LAN to Internet.
YES: Allowed ; **NO:** Blocked ; **N/A:** Not Applicable

Packet Filter – Add TCP/UDP Filter



Rule Name: Specify a User-defined description identifying this entry or click Helper to select existing predefined rules. The maximum name length is 32 characters.

Time Schedule: This is the user-defined time period applicable to the rule. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Selecting the **Subnet Mask** of the IP address range you wish to allow/block the traffic to or form; set IP address and Subnet Mask to **0.0.0.0** to inactive the Address-Filter rule. (such as when you are setting up a port filter rule that is applicable to all hosts)

> ***Tip:*** To block access, to/from a single IP address, enter that IP address as the **Host IP Address** and use a **Host Subnet Mask** of "255.255.255.255".

Type: It is the packet protocol type used by the application, select **TCP**, **UDP** or both **TCP/UDP**.

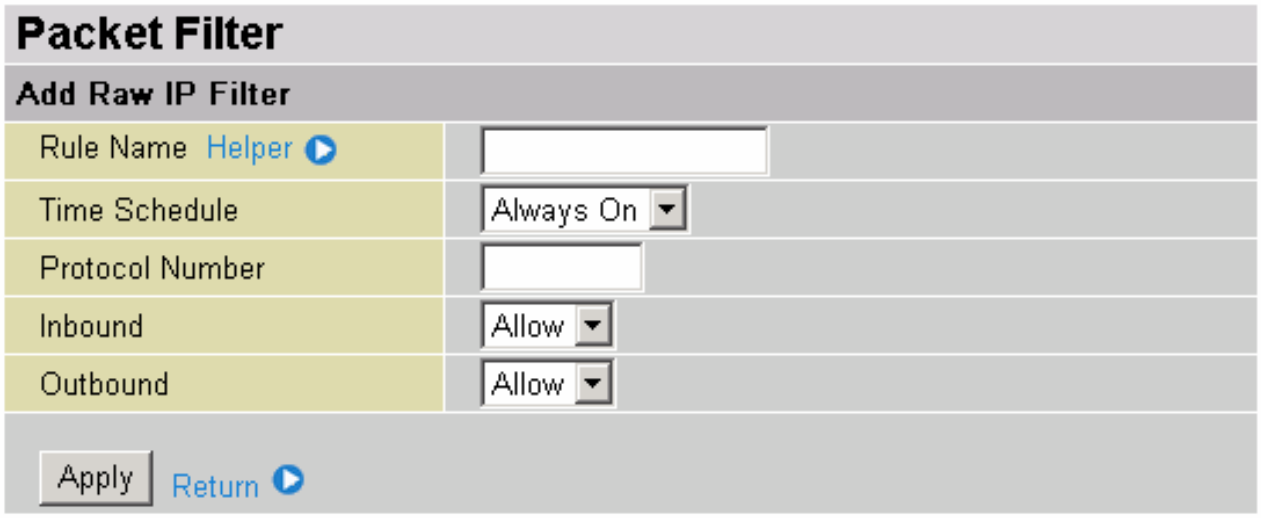
Source Port: This Port or Port Range defines the port allowed to be used by the Remote/WAN to connect to the application. The default is **0 ~ 65535.** It is recommended that this option only be configured by advanced users.

Destination Port: This is the Port (or Port Range) that is defined by the application.

Inbound / Outbound: Select **Allow** or **Block** to control access to the Internet (**"Outbound"**) or from the Internet (**"Inbound"**).

Click the **Apply** button to apply your changes.

Packet Filter – Add Raw IP Filter



Rule Name: Specifies a user-defined description identifying this entry or click Helper to select existing predefined rules.

Time Schedule: this is the user-defined time period applicable to the rule. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section

Protocol Number: Insert the port number, i.e. GRE 47.

Inbound / Outbound: Select **Allow** or **Block** to control access to the Internet (**"Outbound"**) or from the Internet (**"Inbound"**).

Click the **Apply** button to apply your changes.

Example: Configuring your firewall to allow for a publicly accessible web server on your LAN

The predefined port filter rule for HTTP (TCP port 80) is the same no matter whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

As you can see from the diagram below, when the firewall is enabled with one of the three presets (Low/Medium/High), inbound HTTP access is not allowed which means remote access through HTTP to your router is not allowed.

Note: Inbound indicates accessing from Internet to LAN and Outbound is from LAN to the Internet.

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
mei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete
mei_smtp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 25 ~ 25	Block Allow	Edit	Delete
mei_pop3	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 110 ~ 110	Block Allow	Edit	Delete
mei_nntp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 119 ~ 119	Block Allow	Edit	Delete

Configuring Packet Filter:

1. Click **Port Filters**. You will then be presented with the predefined port filter rules screen (in this case, for the low security level) shown below:
   Note: You may edit the predefined rule instead of deleting it. This is an example showing to how you add a filter on your own.

Packet Filter

Add TCP/UDP Filter | Add Raw IP Filter

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
mei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete

Click Delete

2. Click **Delete** to delete the existing HTTP rule.
3. Click **Add TCP/UDP Filter**.

Click Add TCP/UDP Filter

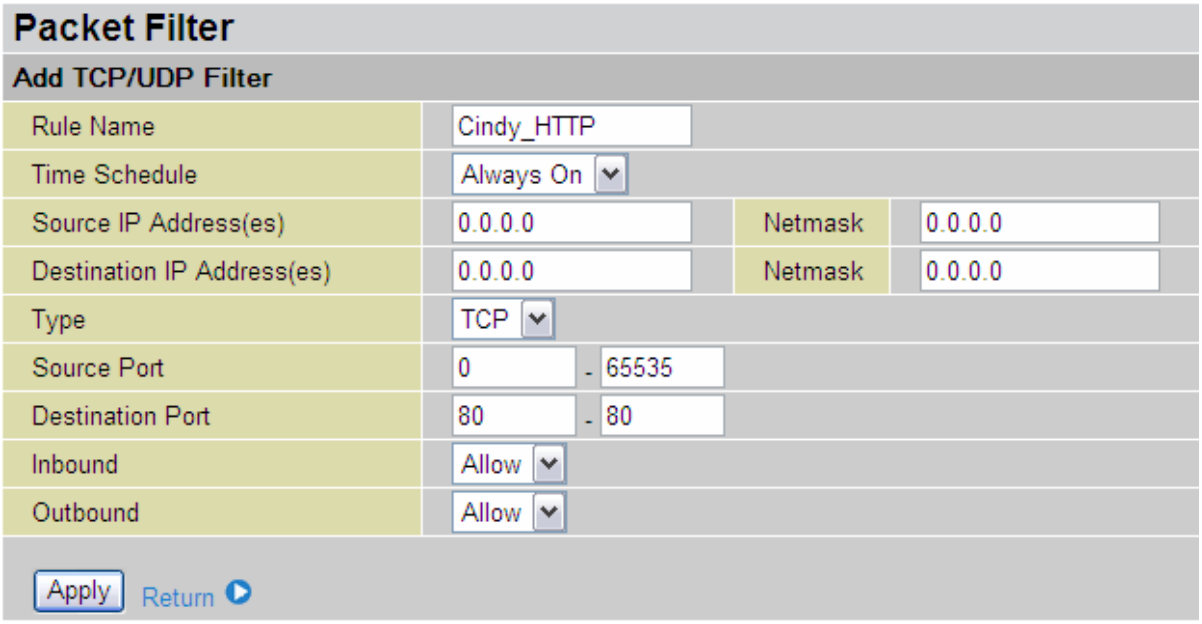
Packet Filter

Add TCP/UDP Filter | Add Raw IP Filter

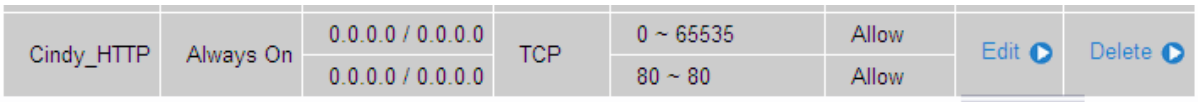
4. Input the Rule Name, Time Schedule, Source/Destination IP, Type, Source/Destination Port, Inbound and Outbound.

   ***Example*:**

   Application: *Cindy_HTTP*
   Time Schedule: *Always On*
   Source / Destination IP Address(es): *0.0.0.0* ***(I do not wish to active the address-filter, instead I use the port-filter)***
   Type: *TCP (Please refer to Table1: Predefined Port Filter)*
   Source Port: *0-65535* ***(I allow all ports to connect with the application))***
   Redirect Port: *80-80* ***(This is Port defined for HTTP)***
   Inbound / Outbound: *Allow*

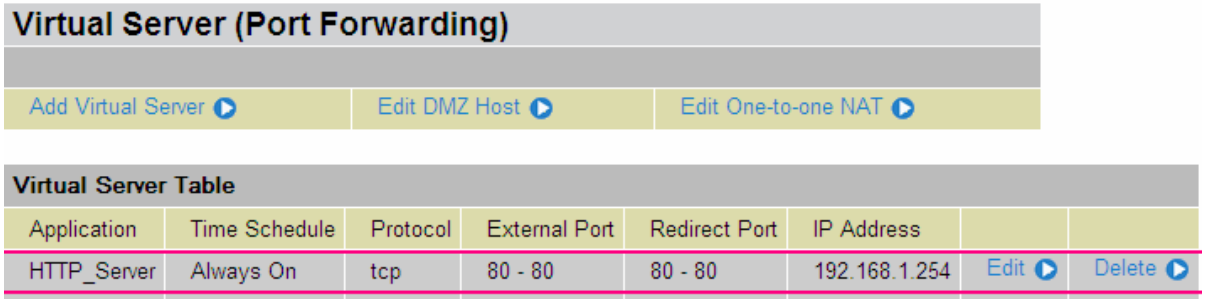


5. The new port filter rule for HTTP is shown below:

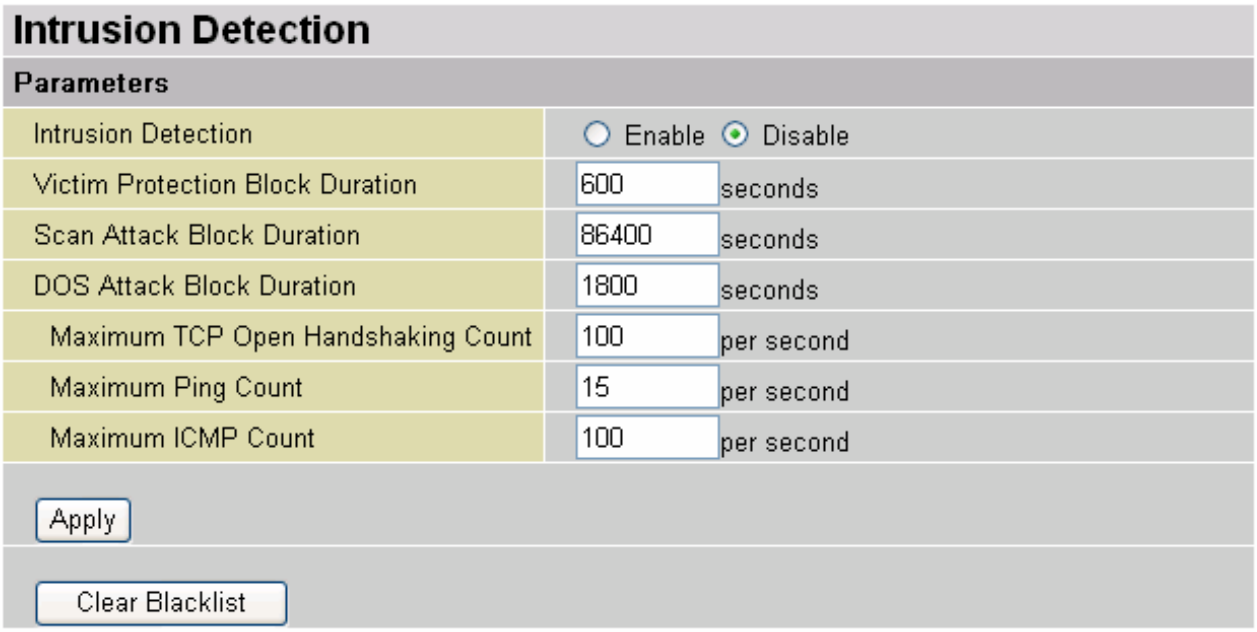


6. Configure your Virtual Server ("port forwarding") settings so that incoming HTTP requests on port 80 will be forwarded to the PC running your web server:

Note: For how to configure the HTTP in Virtual Server mode , go to **Add Virtual Server** in the **Virtual Server** section for more details.



Intrusion Detection



The router's *Intrusion Detection System* (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified as the **Block Duration**. The default setting for this function is **disable.** Some attack types are denied immediately without using the Blacklist function, such as *Land attack* and *Echo/CharGen scan*.

Intrusion Detection: If enabled, IDS will block Smurf attack attempts. Default is **disable**.

Block Duration:

- **Victim Protection Block Duration**: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.
- **Scan Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.
- **DoS Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

Max TCP Open Handshaking Count: This is a threshold value to decide whether a *SYN Flood* attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an *ICMP Echo Storm* is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an *ICMP flood* is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

For *SYN Flood*, *ICMP Echo Storm* and *ICMP flood*, IDS will just warn the user in the Event Log. The router cannot protect against such attacks.

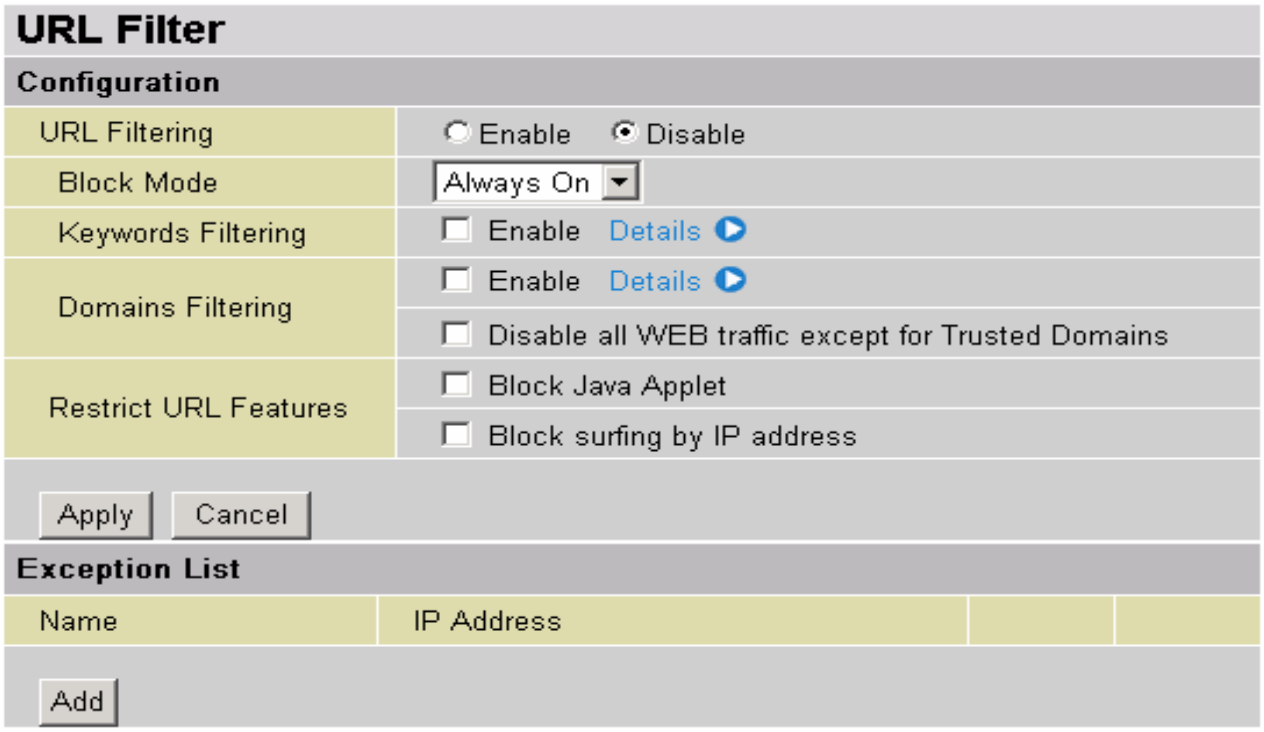
Table 2: Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Src Port: Source Port
Dst Port: Destination Port
Dst IP: Destination IP

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Enable/Disable: To enable or disable the URL Filter feature.

Block Mode: A list of the URL filter rule time modes from which you can choose . The default is set to **Always On.**

- **Disabled:** No action will be performed by the Block Mode.
- **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.
- **TimeSlot1 ~ TimeSlot16:** these are user-defined time periods. You may specify the time period during which the URL filter rules apply, i.e. during working hours. For setup and details, refer to **Time Schedule** section.

Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is http://www.abc.com/abcde.html, it will be dropped if the keyword “abcde” occurs in the URL.

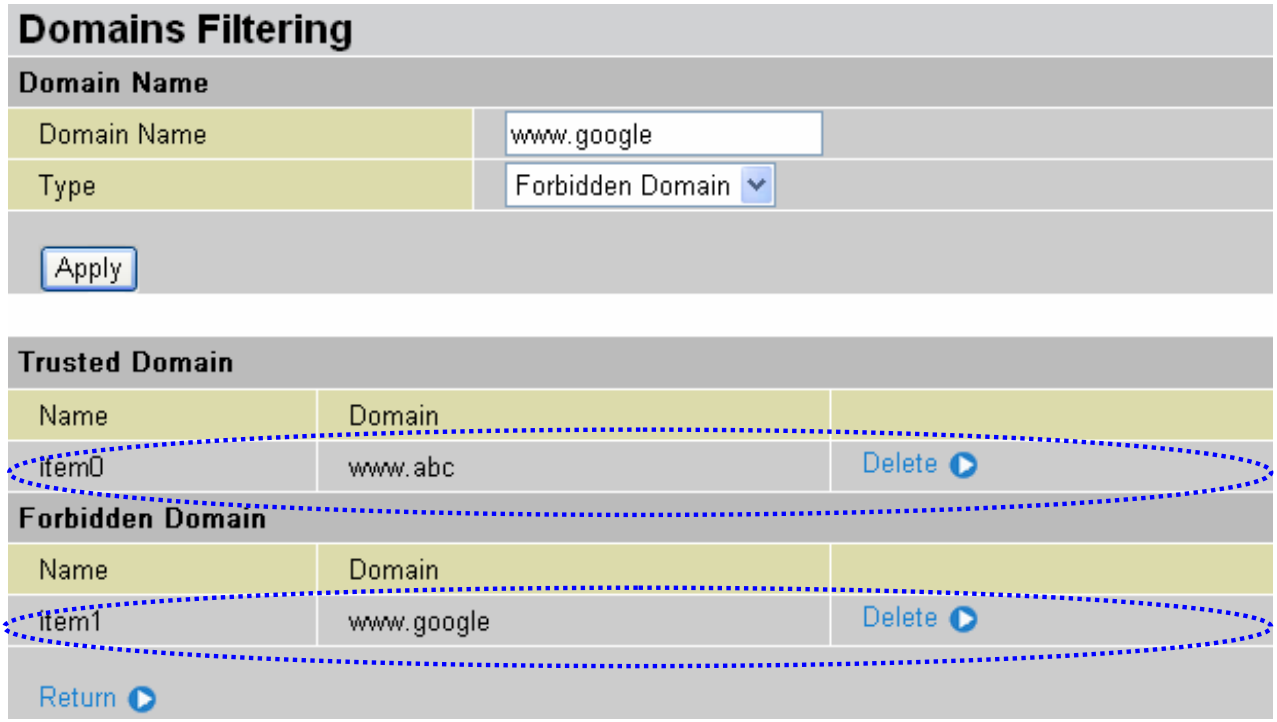
Domains Filtering: This function checks the whole URL (not the IP address) in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. The router checks the domain in the URL to determine if it is in the trusted list. If it is, the connection attempt is sent to correct the remote web server.
2. If not, the router checks if the domain is listed in the forbidden list. If it is, then the

connection attempt will be dropped.

3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please note that the completed URL, "www" + domain name should be specified. For example to block traffic to www.google.com.au, enter "www.google" or "www.google.com"

In the example below, the URL request for www.abc.com will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.google or www.google.com will be dropped, because www.google is in the forbidden list.



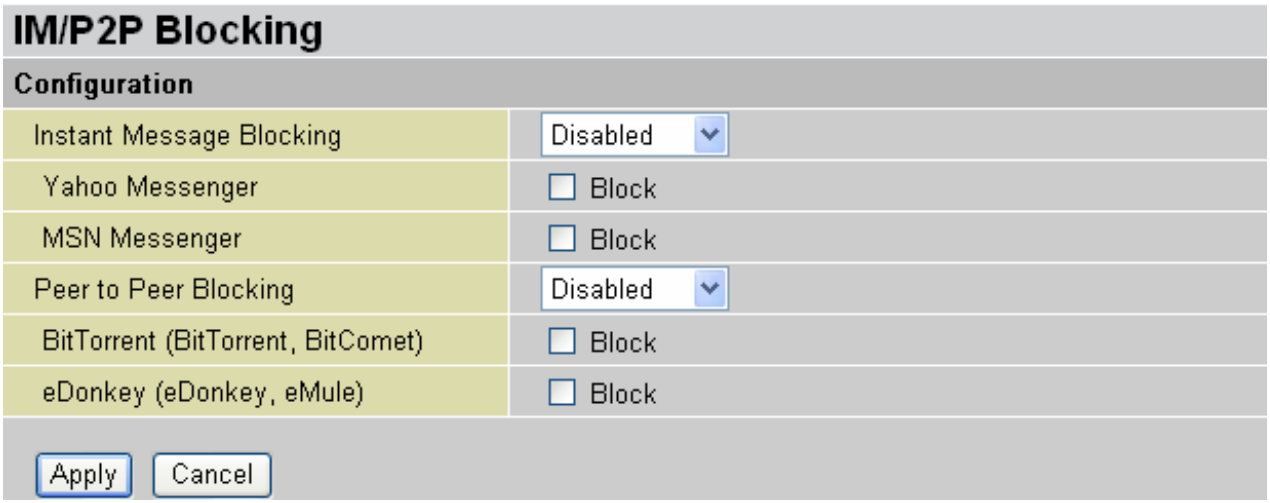
Example: Andy wishes to disable all WEB traffic except for ones listed in the trusted domain, which would prevent Bobby from accessing other web sites. Andy selects both check boxes in ***Domain Filtering*** and thinks that this will stop Bobby. But Bobby knows this function, *Domain Filtering*, ONLY disables all WEB traffic except for **Trusted Domain,** BUT not connections using **IP addresses.** In this situation, the **Block surfing by IP address** function can be handy and helpful to Andy. Now, Andy can prevent Bobby from accessing sites, both by IP and by domain name.

Restrict URL Features: This function enhances your URL rules.

- **Block Java Applet:** This function can block Web content that includes a Java Applet. This is to prevent someone who wants to damage your system via standard HTTP protocol.
- **Block surfing by IP address:** This prevents someone who uses the IP address as URL from skipping the Domains Filtering function. This is only Activate if Domain Filtering is enabled.

IM / P2P Blocking

IM, short for Instant Messaging, is required to use client program software that allows users to communicate, exchanging text message, with other IM users, in real time, over the Internet. A P2P application, known as Peer-to-Peer, is a group of computer users who share files to specific groups of people across the Internet. Both Instant Messaging and Peer-to-Peer applications make communication faster and easier, but your network can become increasingly insecure at the same time. This router's IM and P2P blocking system helps users to restrict LAN computers from access to the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.



Instant Message Blocking: The default is **Disabled.**

- **Disabled:** The Instant Messaging blocking function is not activated. No blocking will be Performed.
- **Always On:** The Instant Messaging blocking function is activated. Blocking is enabled.
- **TimeSlot1 ~ TimeSlot16:** These are user-defined time periods. You may specify the time period during which the blocking is active, i.e. during working hours. For setup and details, refer to **Time Schedule** section.

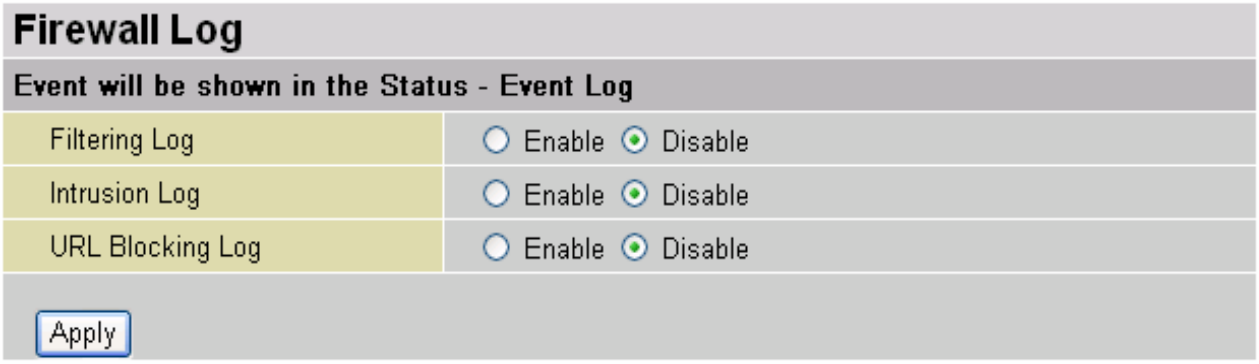
Yahoo/MSN Messenger: Select this box to block either Yahoo and/or MSN Messenger. Be sure that you have enabled the *Instant Message Blocking* first.

Peer to Peer Blocking: The default is **Disabled.**

- **Disabled:** The Instant Messaging blocking function is not active. No connections will be blocked
- **Always On** The Instant Messaging blocking function is activated. Blocking is enabled.
- **TimeSlot1 ~ TimeSlot16:** These are user-defined time periods. You may specify the time period during which the blocking is active, i.e. during working hours. For setup and details, refer to **Time Schedule** section.

BitTorrent / eDonkey: Select this box to block either Bit Torrent and/or eDonkey. To be sure you have first enabled the *Peer to Peer Blocking* function.

Firewall Log



The Firewall Log displays log information of any unexpected action with your firewall settings.

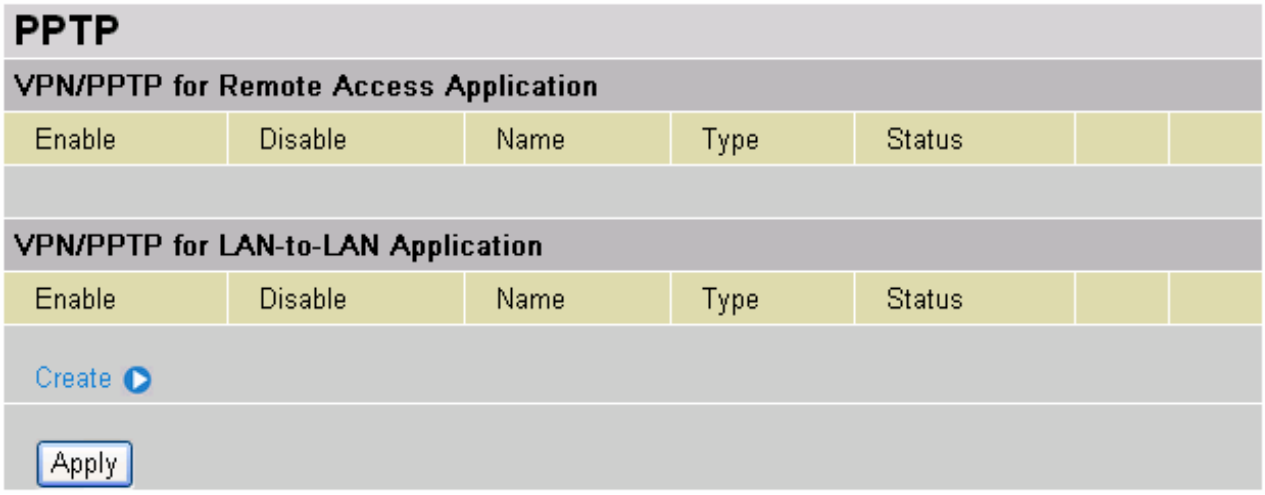
Select the **Enable** box to activate the logging.

Log information can be seen in the **Status – Event Log** screen after enabling.

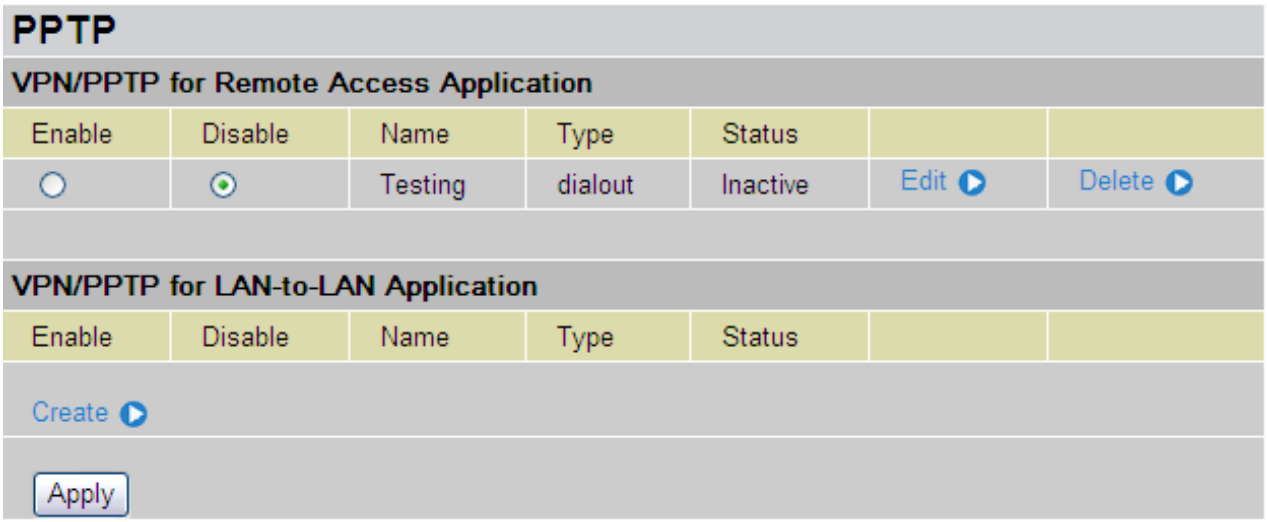
VPN - Virtual Private Networks

Virtual Private Networks are a way to establish secured communication tunnels to an organization's network via the Internet. Your router supports three main types of VPN (Virtual Private Network), **PPTP**, **IPSec** and **L2TP.**

PPTP (Point-to-Point Tunneling Protocol)



There are two types of PPTP VPN's supported; **Remote Access** and **LAN-to-LAN** (Please read below for more information.). Click **Create** to configure a new VPN connection.



After you have created PPTP connection, it's account status will be displayed. (See example above).

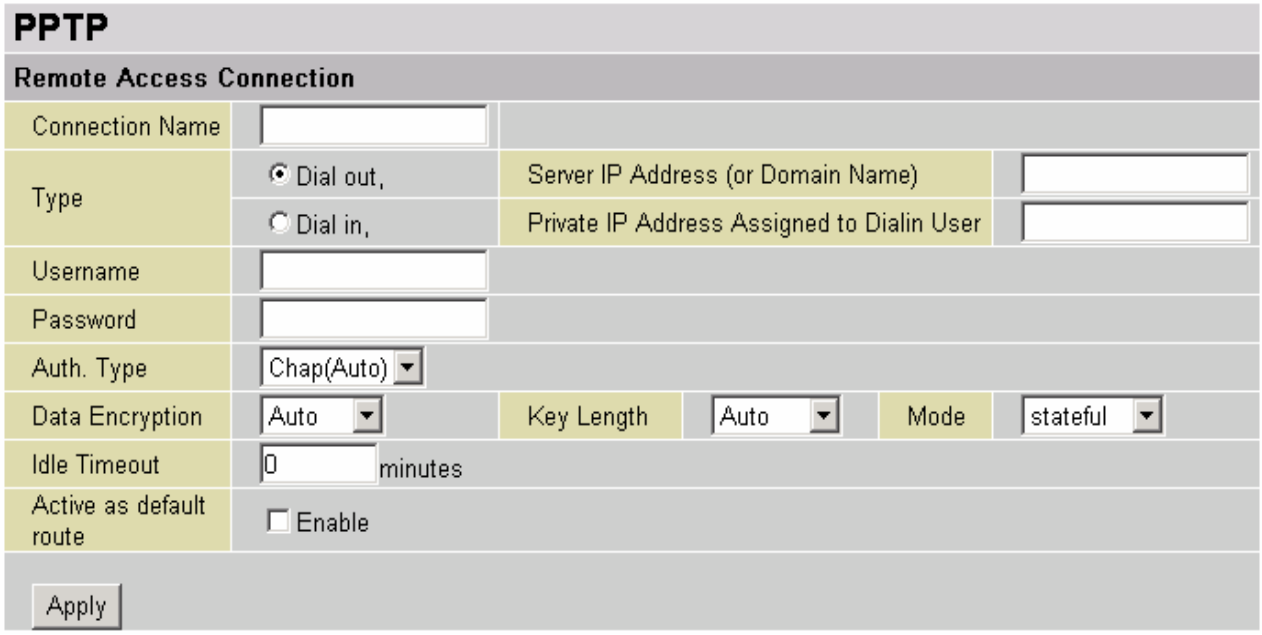
⊙ **Enable / Disable:** This function activates or deactivates the PPTP connection. If you wish to disable the tunnel, select the **Disable** radio button and click on the **Apply** button to deactivate the connection.

Name: The user-defined name of the connection.

Type: This refers to your whether your router operates as a client or a server, select eather **Dialout** for client, or **Dialin** for server.

Status: This informs you of your PPTP tunnel connection condition.

PPTP Connection - Remote Access



Connection Name: A user-defined name for the connection (e.g. “connection to office”).

Type: Select **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), select **Dial In** if you want your router to operate as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Domain Name)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto.** This is the correct setting if you want the router to determine which authentication type to use, or else you can manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client) When acting as a server, specify the authentication type you want clients connecting to your router to use. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the original client.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto** and this means that this setting is negotiated when establishing a connection. Alternativly, you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto** which means that it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

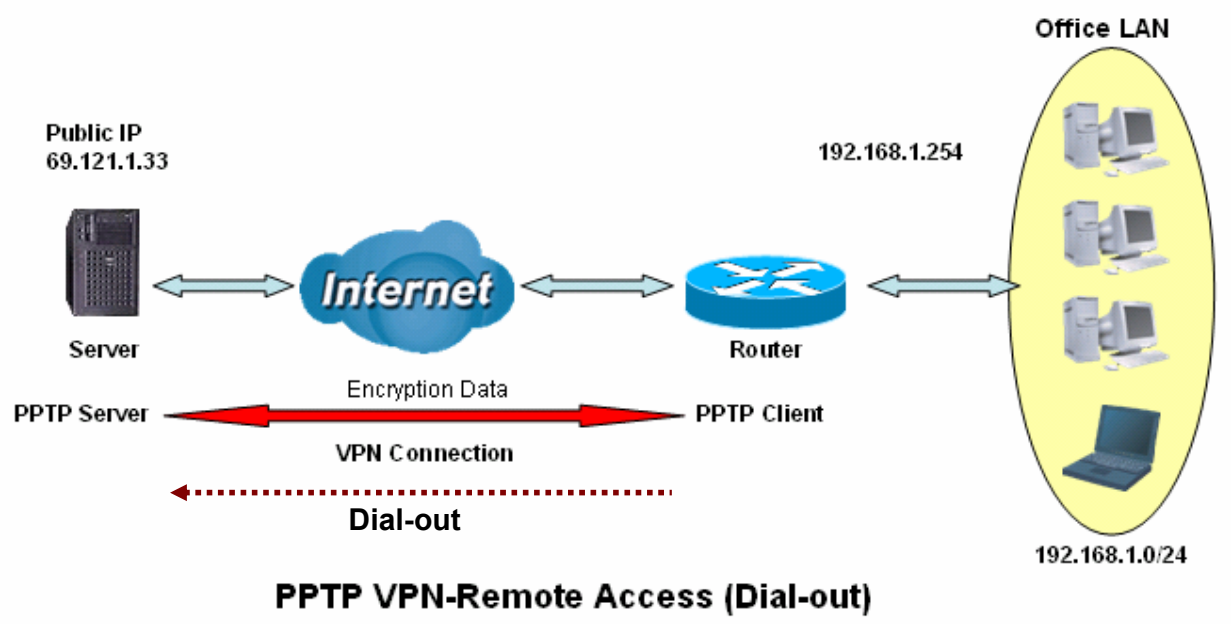
Active as default route: If you select this option while using *Dial-out* connection, all packets will route through the VPN tunnel to the Internet; therefore, activating the function may degrade Internet

performance.

Click **Apply** button to apply your changes.

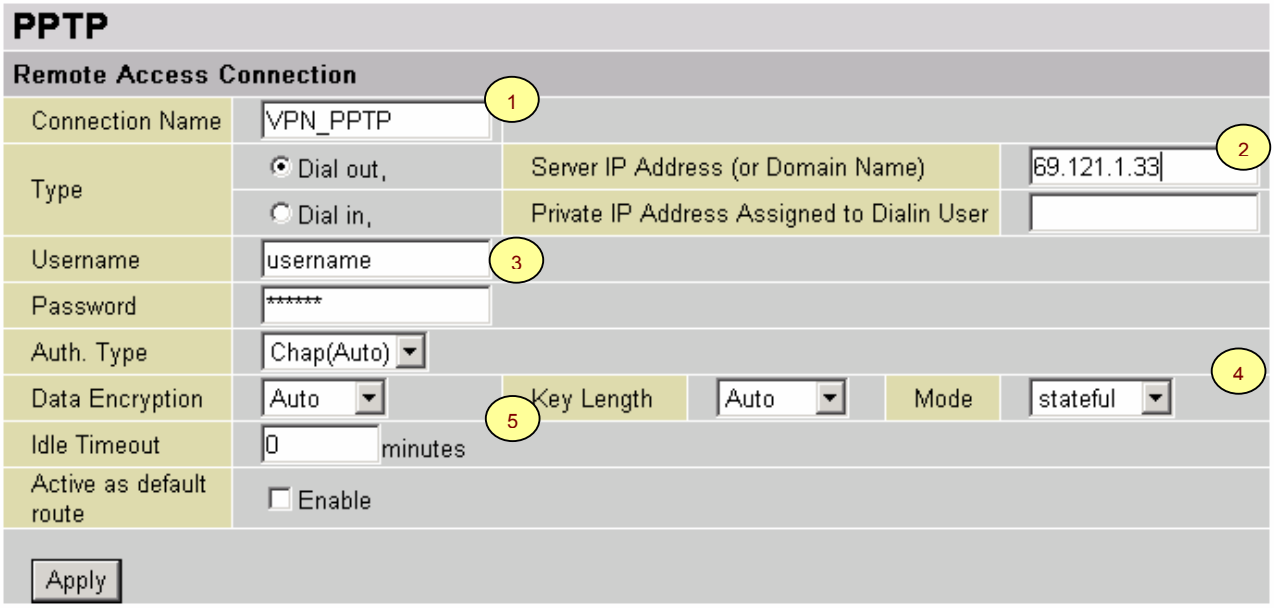
Example: Configuring a Remote Access PPTP VPN Dial-out Connection

A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, and connected to a couple of PCs and Servers.



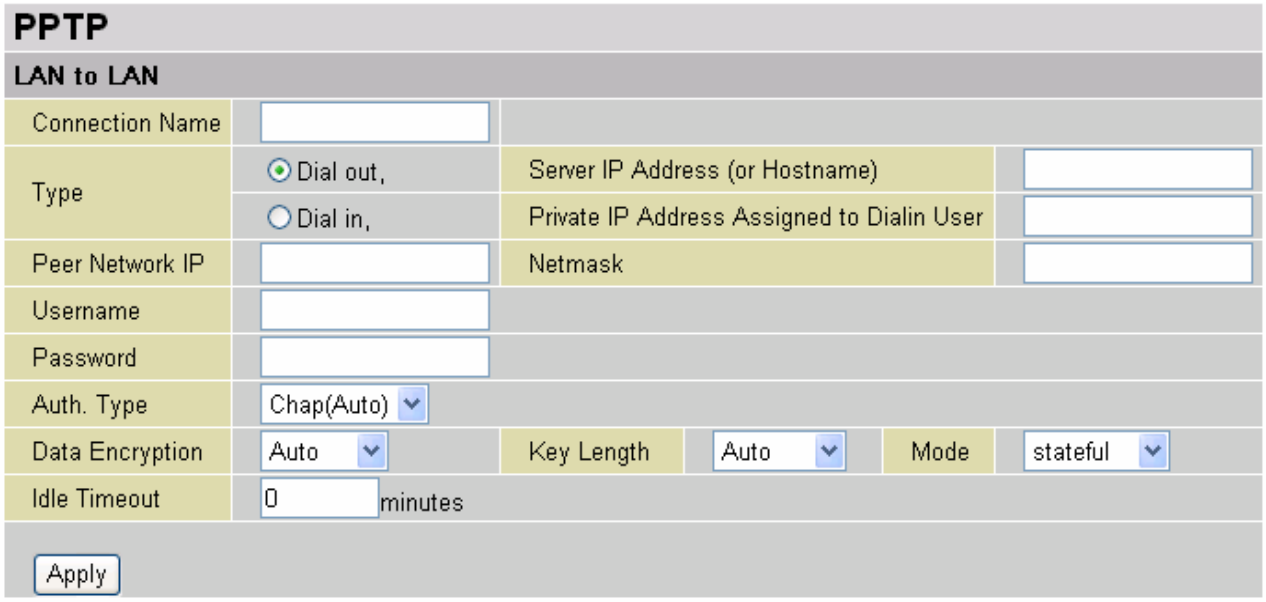
Configuring the PPTP VPN in the Office

You can either input the IP address (69.1.121.33 in this case) or hostname to reach the server.



Item	Function		Description
1	Connection Name	VPN_PPTP	Given name of PPTP connection
2	Dial out		Select **Dial out**
	Server IP Address (or Hostname)	69.121.1.33	The Dialed server's IP
3	Username	username	Your username & password to access the server
	Password	123456	
4	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to the relevant section of this manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
5	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always on.

PPTP Connection - LAN to LAN



Connection Name: User-defined description of the connection.

Type: Select **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server) or select **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto.** Retain this setting if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), When acting as a server, select the authentication type you want clients connecting to you to use. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the original client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection. Alternativly, you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, which negotiates the that is used when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

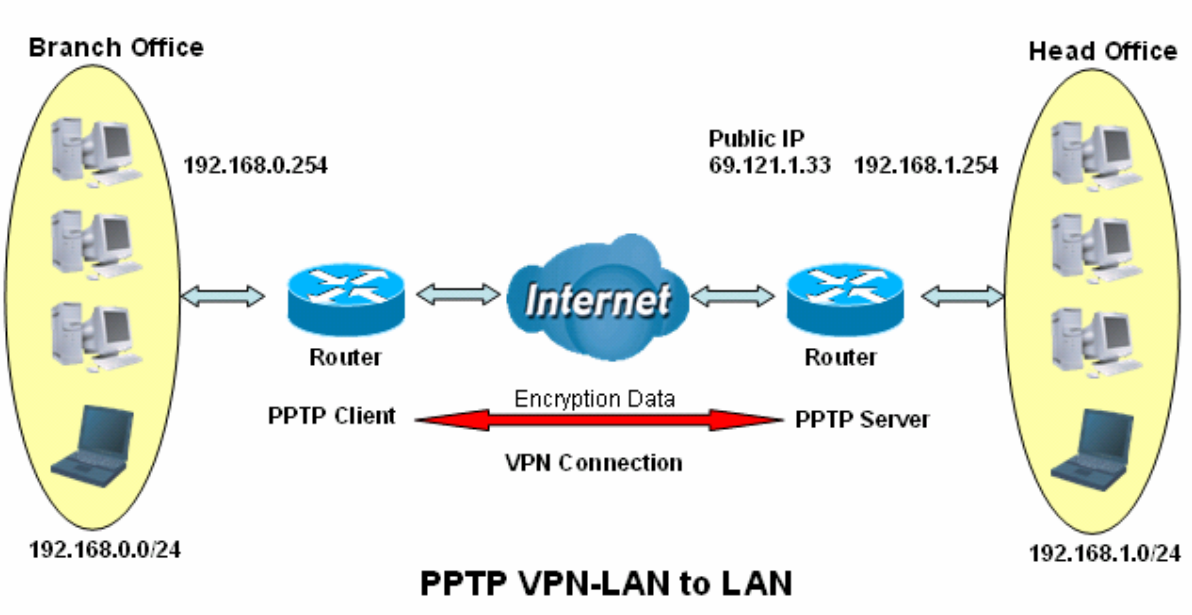
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnects the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Click **Apply** button to apply your changes.

Example: Configuring a PPTP LAN-to-LAN VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

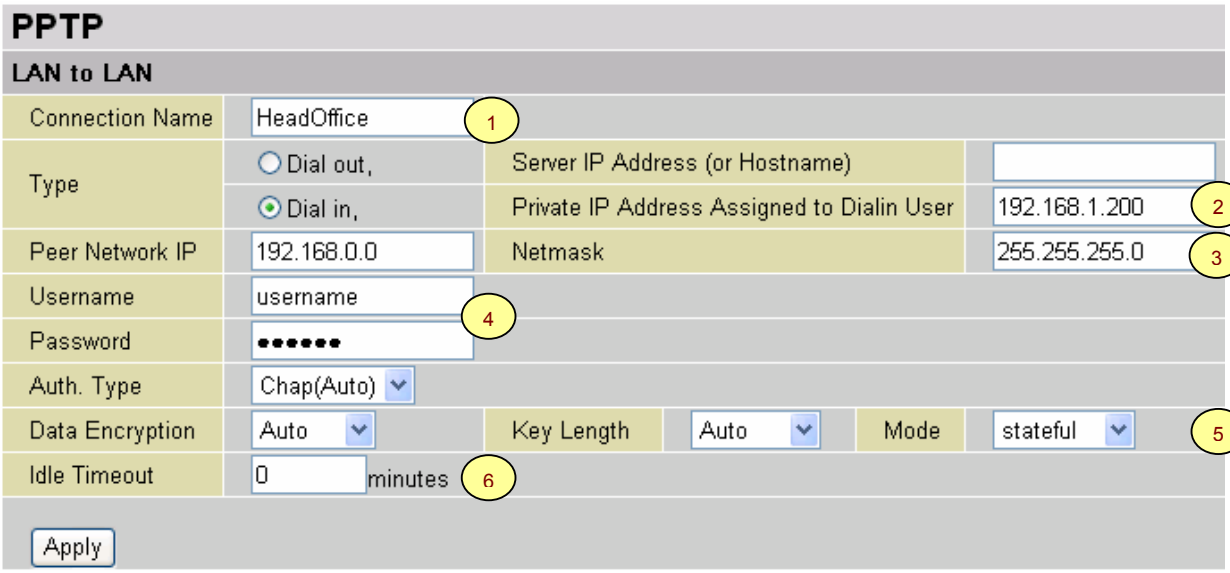


Attention

Both office LAN networks **MUST in different subnet** when using the LAN to LAN application.

Configuring PPTP VPN in the Head Office

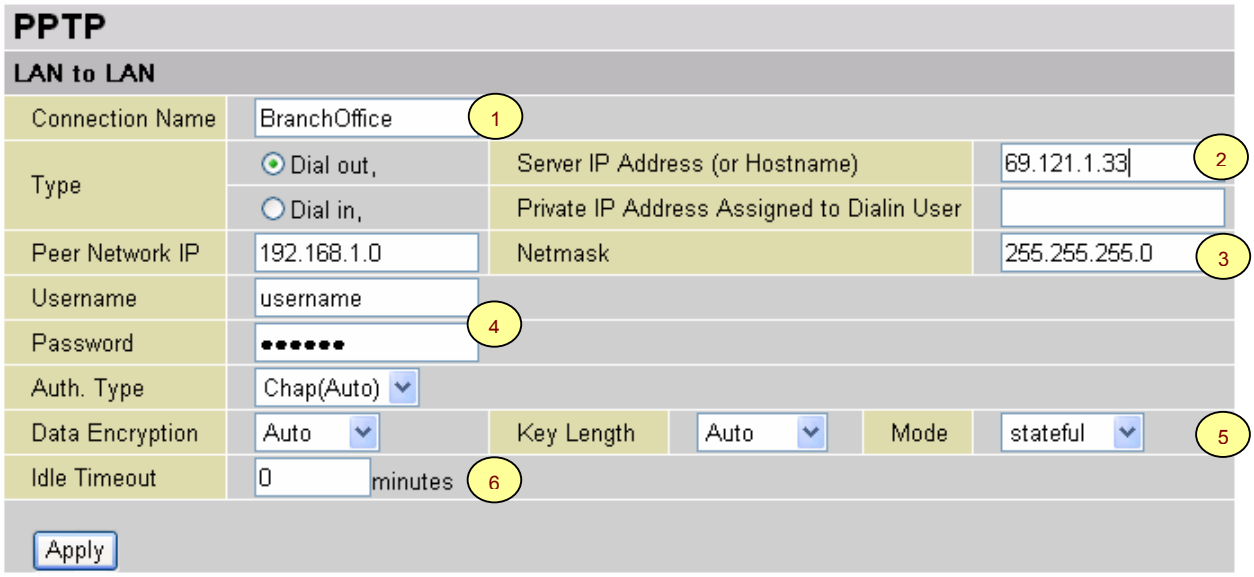
The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Connection Name	HeadOffice	Given name of the PPTP connection
2	Dial in		Select Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	IP address assigned to branch office network
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to this manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.

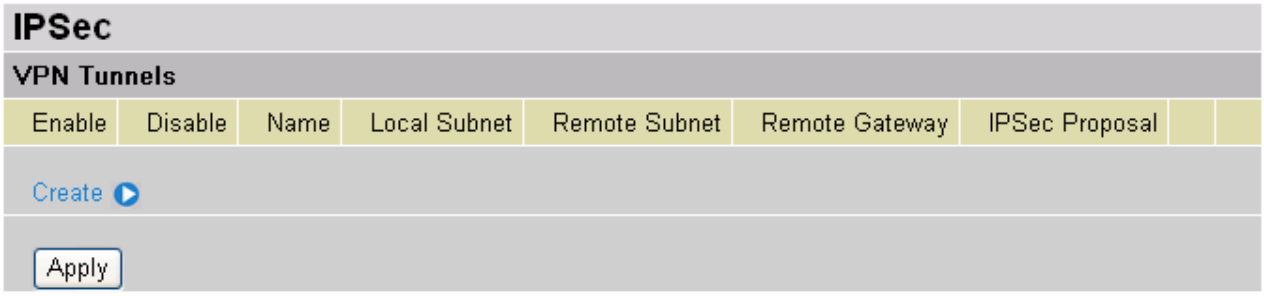
Configuring PPTP VPN in the Branch Office

The IP address 69.1.121.30 is the **Public IP** address of the router located in head office. If you registered a DDNS account (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.

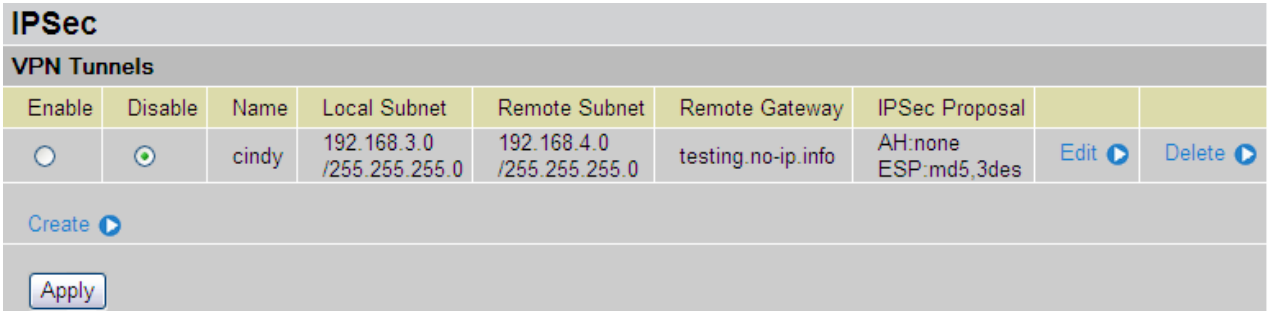


Item	Function		Description
1	Connection Name	BranchOffice	Given name of the PPTP connection
2	Dial out		Select Dial out
	Server IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to this manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.

IPSec (IP Security Protocol)



Click **Create** to create a new IPSec VPN connection account.



After you have created the IPSec connection, account information will be displayed. (See example above).

Enable / Disable: This function activates or deactivates the IPSec connection. If you wish to disable the tunnel, select **Disable** and click **Apply** to deactivate the connection.

Name: This is the user-defined name of the connection.

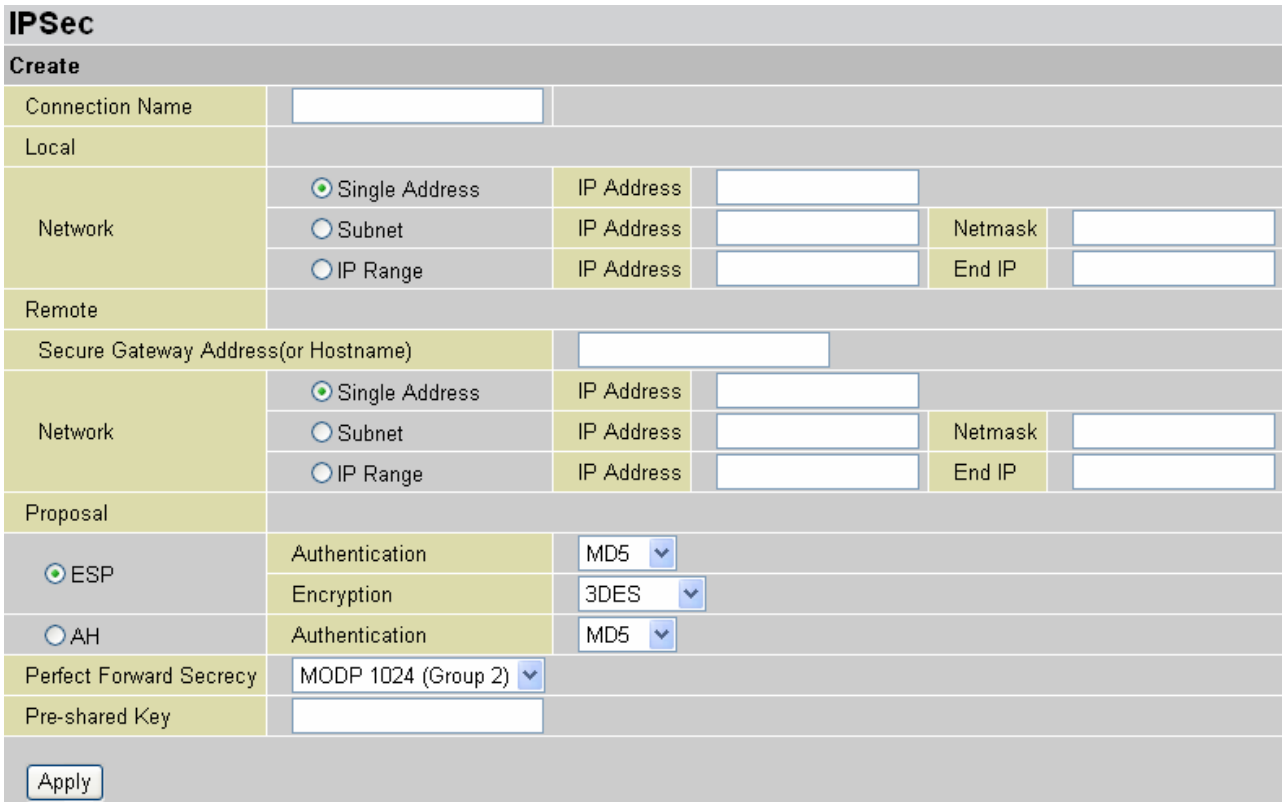
Local Subnet: Displays the IP address and subnet of the local network.

Remote Subnet: Displays the IP address and subnet of the remote network.

Remote Gateway: This is the IP address or Domain Name of the remote VPN device that is to be connected and establish a VPN tunnel.

IPSec Proposal: This is selected IPSec security method.

IPSec VPN Connection



Connection Name: The user-defined name for the connection (e.g. “connection to office”).

Local Network: Set the IP address, subnet or address range of the local network.

- **Single Address:** The IP address of the local host.
- **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).
- **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10.

Remote Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is to be connected to when establishing a VPN tunnel.

Remote Network: Set the IP address, subnet or address range of the remote network.

Proposal: Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with during transmission. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES**, **AES (128, 192 and 256)** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

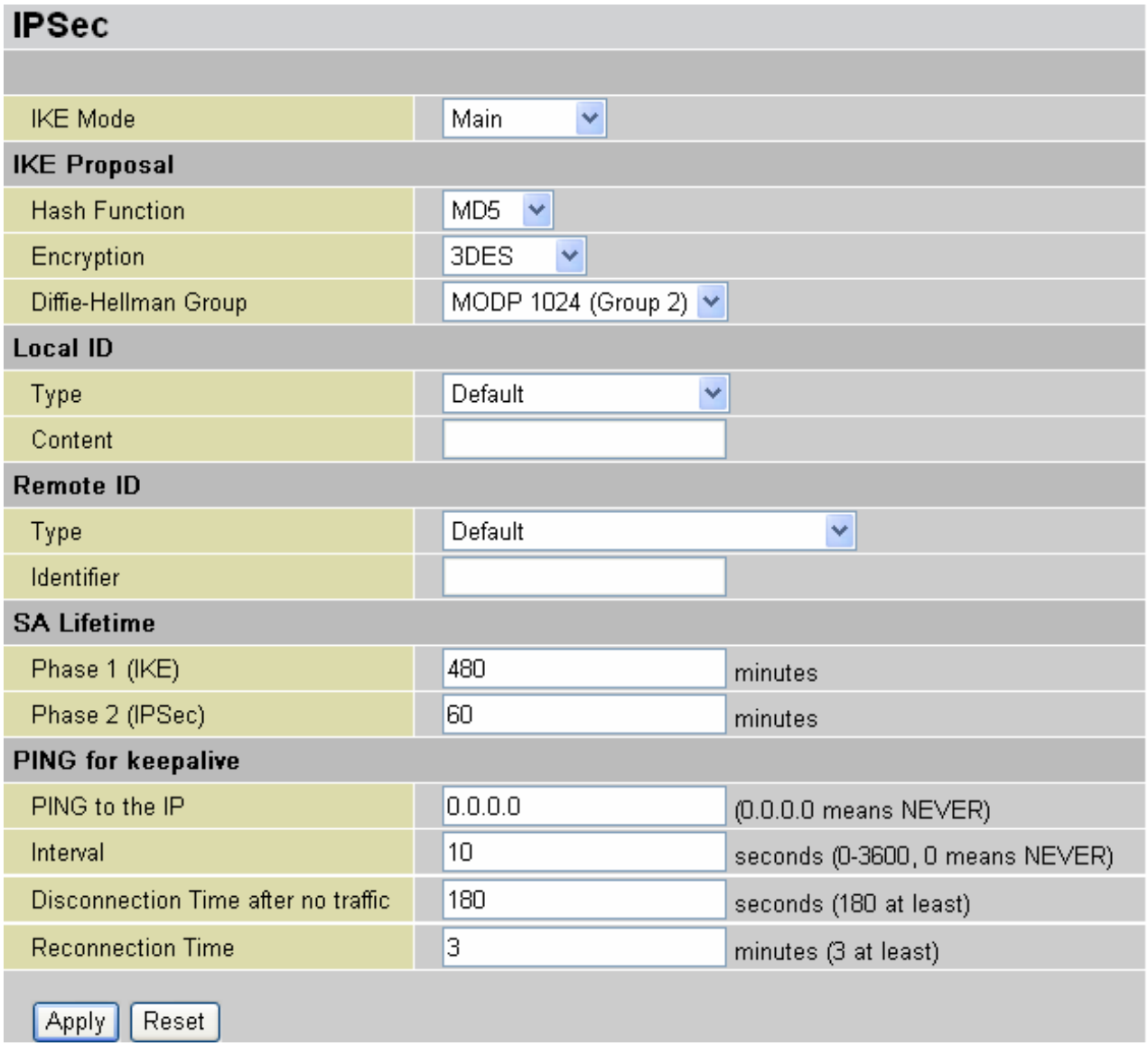
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Select the **Apply** button to apply your changes.

Advanced Option

This function is only available after completely creating an IPSec account. Click **Advanced Option** to change the following settings:



IKE (Internet key Exchange) Mode: Select IKE mode to Main mode or Aggressive mode. This IKE provides secured key generation and key management.

IKE Proposal:

Hash Function: This is a Message Digest algorithm which coverts any length of a message into a unique set of bits. You can use either MD5 (Message Digest) or SHA-1 (Secure Hash Algorithm) algorithms. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES** and **AES (128, 192 and 256)**. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Local ID:

- **Type:** Specify local ID type.
- **Content:** Input ID's information, like domain name www.ipsectest.com.

Remote ID:

- **Type:** Specify Remote ID type.
- **Identifier:** Input remote ID's information, like domain name www.ipsectest.com.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

- **Phase 1 (IKE): U**sed to issue an initial connection request for a new VPN tunnel. Any value can be selected between 5 and 15,000 minutes. The default is 480 minutes.
- **Phase 2 (IPSec):** Used to negotiate and establish secure authentication. Any value can be selected between 5 and 15,000 minutes. The default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Ping to Keep Alive:

PING to the IP: The router is able to IP Ping the remote PC with a specified IP address and alert the user when the connection fails. Once the alert message is received, the router will drop this tunnel connection. The connection will need to be re-established. Default setting is 0.0.0.0 which disables this function.

Interval: This sets the time interval between ***Pings to the IP*** function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set to any value between 0 and 3600 seconds, 0 second disables this function.

Ping to the IP	Interval (sec)	*Ping to the IP* Action
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (Any valid IP Address)	0	No
xxx.xxx.xxx.xxx(Any valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after no traffic: This is the "NO Response" timer. When no traffic is received for more than the Disconnection time setting, the router will automatically halt the tunnel connection and re-establish it base after the **Reconnection Time** has elapsed. **180 seconds** is minimum time interval for this function.

Reconnection Time: This is the reconnecting time interval after the NO TRAFFIC timeout has occurred. **3 minutes** is minimum time interval for this function.

Select the **Apply** button to update the settings.

Example: Configuring a IPSec LAN-to-LAN VPN Connection

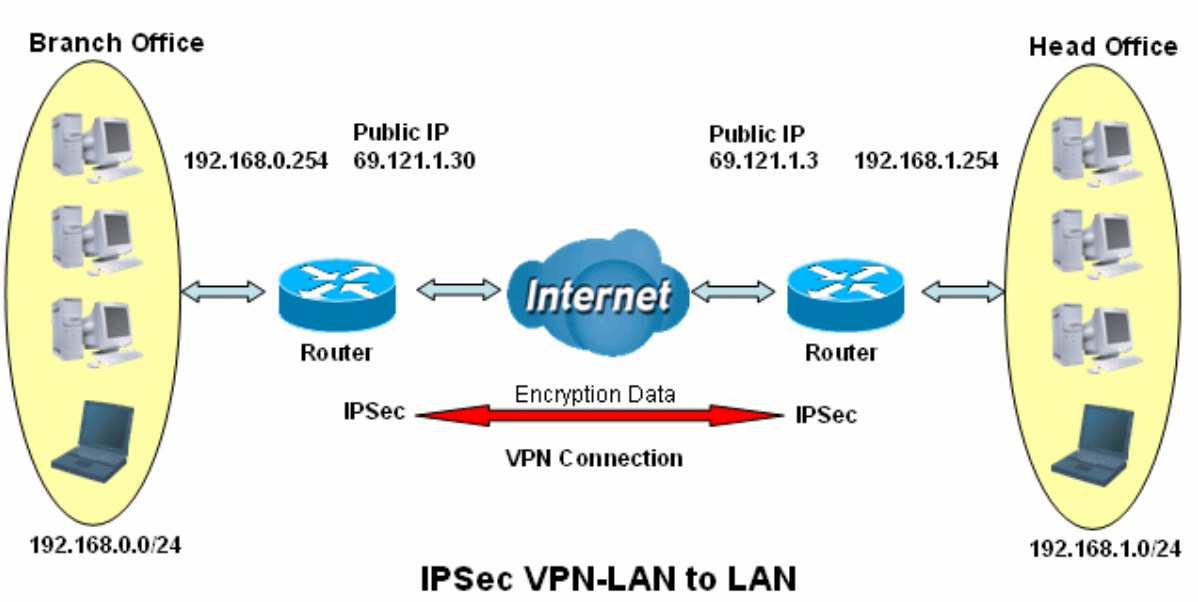


Table 3: Network Configuration and Security Plan

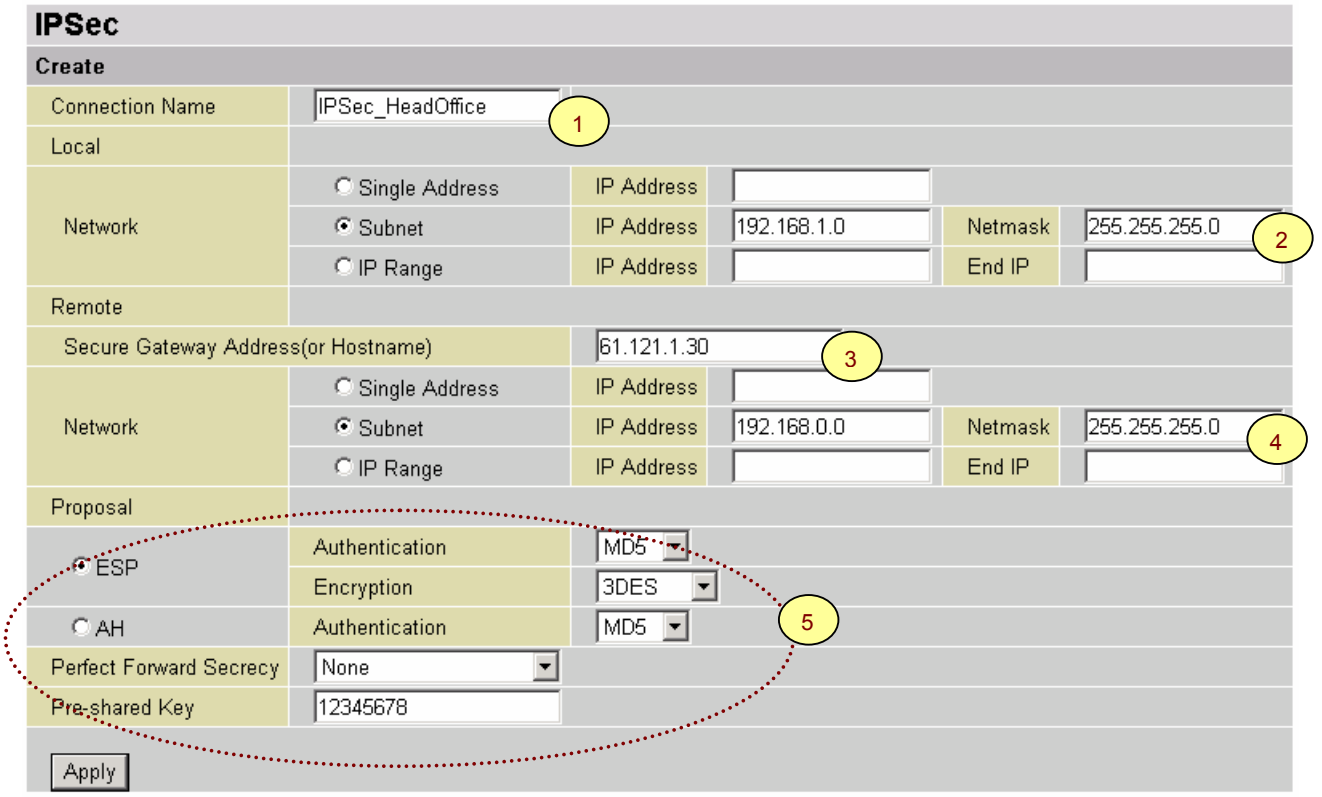
	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.1.121.30	69.1.121.3
Remote Network ID	192.168.1.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Connection Type	Tunnel mode	Tunnel mode
Security Algorithm	ESP:MD5 with AES	ESP:MD5 with AES

Attention

Both office LAN networks **MUST on different subnets** when using the LAN to LAN application.

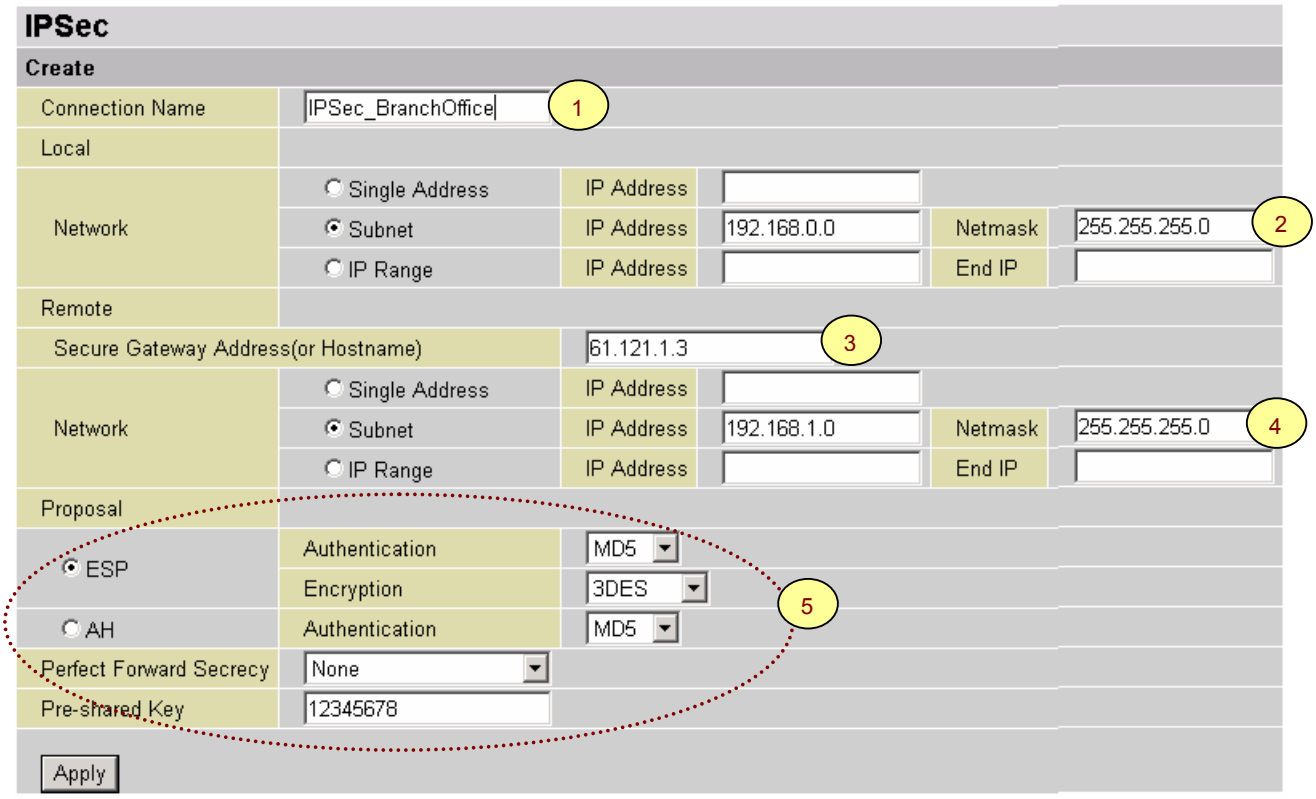
The settings of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring IPSec VPN in the Head Office



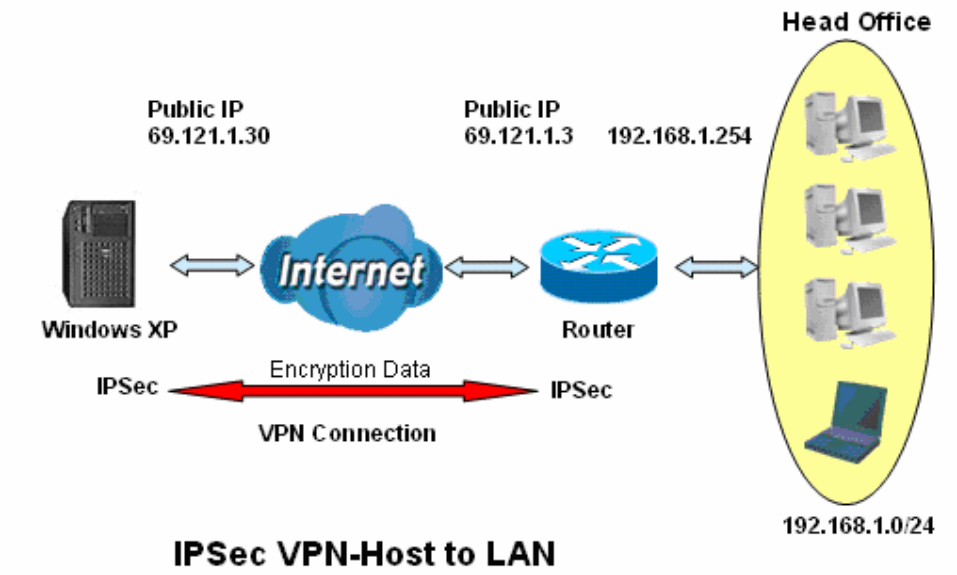
Item	Function		Description
1	Connection Name	IPSec_HeadOffice	Given name of the IPSec connection
2	Subnet		Select the Subnet button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.30	IP address of the head office router (WAN side)
4	Subnet		Select the Subnet button
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	ESP		Select the ESP button
	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

Configuring IPSec VPN in the Branch Office

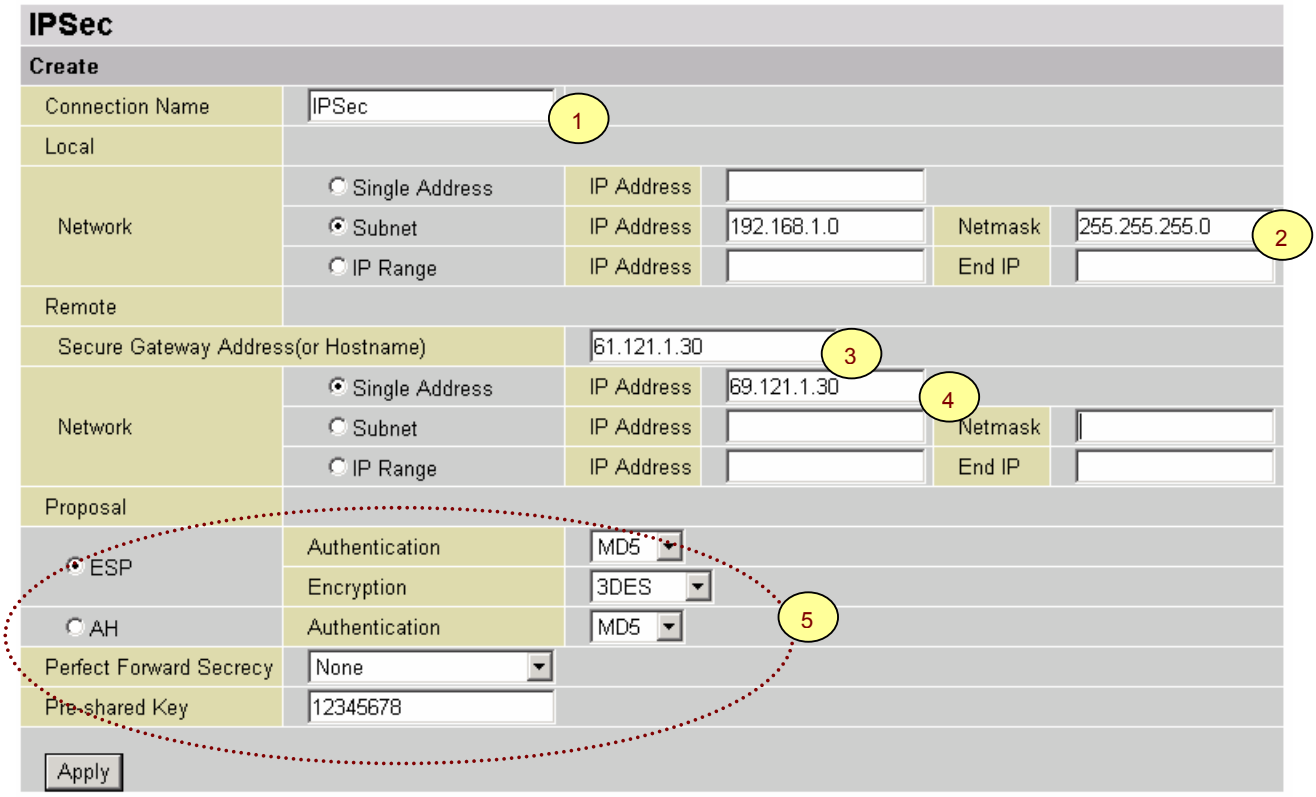


Item	Function		Description
1	Connection Name	IPSec_Branch Office	Given name of the IPSec connection
2	Subnet		Select the Subnet button
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.3	IP address of the head office router (in WAN side)
4	Subnet		Select the Subnet button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	ESP		Select the ESP button
	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

Example: Configuring a IPSec Host-to-LAN VPN Connection

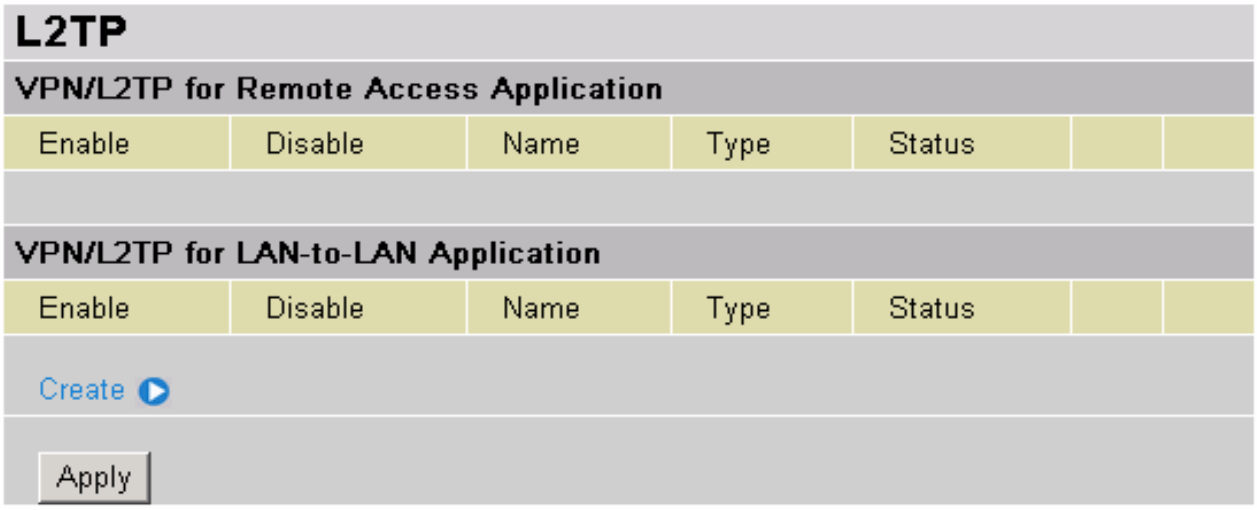


Configuring IPSec VPN in the Office

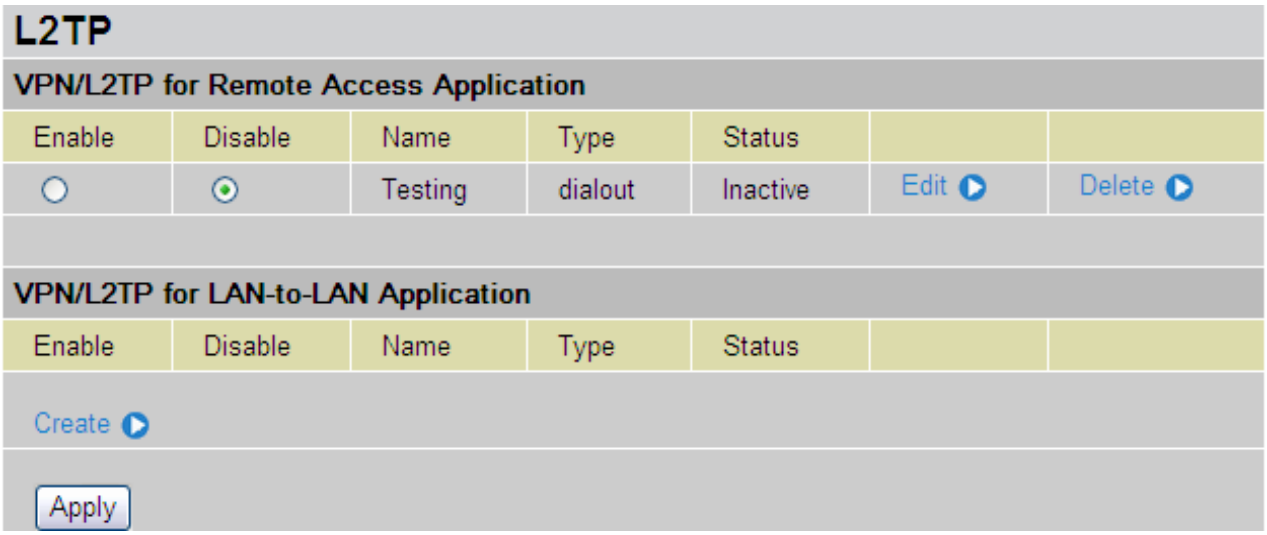


Item	Function		Description
1	Connection Name	IPSec	Given name of the IPSec connection
2	Subnet		Select the Subnet button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
4	Single Address		Select the Single Address button
	IP Address	69.121.1.30	Remote computers IP address
5	ESP		Select the ESP button
	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

L2TP (Layer Two Tunneling Protocol)



Two types of L2TP VPN are supported **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to create a new VPN connection account.



After you have created L2TP connection, the account status will be displayed. (As shown above).

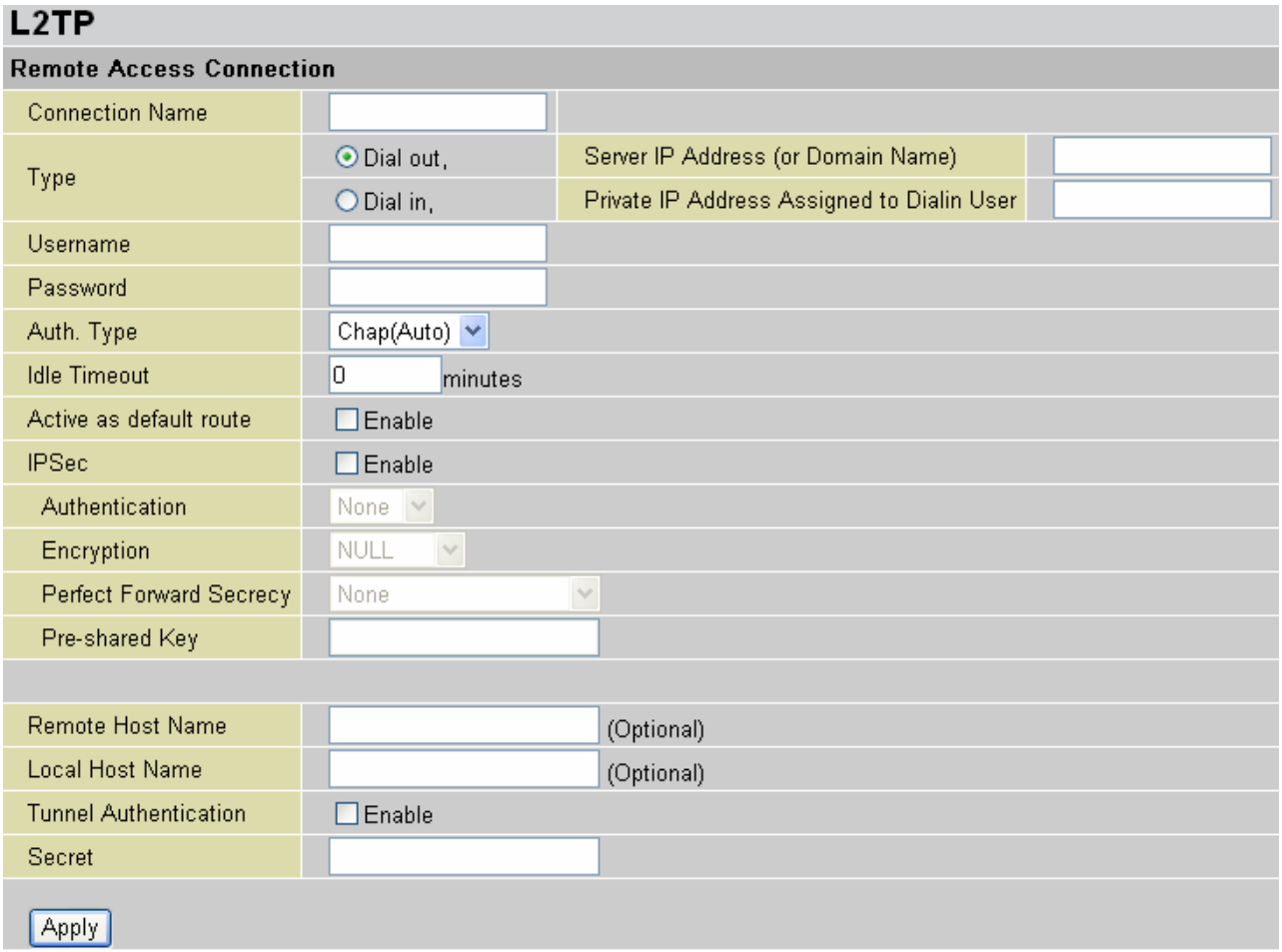
⊙ **Enable / Disable:** This function activates or deactivates the L2TP connection. If you wish to disable the tunnel, select the **Disable** button and click **Apply** to deactivate the connection.

Name: This is the user-defined name of this connection.

Type: This refers to whether your router operates as a client or a server, **Dialout** for client or **Dialin** for server.

Status: This indicates your L2TP tunnel connection status.

L2TP Connection - Remote Access



L2TP VPN Connection

Connection Name: A User-defined name for the connection (e.g. “connection to office”).

Type: Select **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), select **Dial In** if you wish your router to operate as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** that you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** (this is the IP address that the remote client will be assigned when it connects) .

Username: If you are a Dial-Out user (client), enter the username provided by your Host (Your username for the server that you are connecting to) . If you are a Dial-In user (server), enter the username that the connecting client will use to connect to your router.

Password: If you are a Dial-Out user (client), enter the password provided by your Host Your password for the server that you are connecting to). If you are a Dial-In user (server), enter the password that the connecting client will use to connect to your router

PPP Authentication Type: Default is **Auto.** This will allow the router to determine the best suited authentication type. Alternatively, you can manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client) If your router is acting as a server, specify the authentication type you want clients connecting to you to use. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Idle Time: When there is no activity on the connection for this pre-determined Idle time, the VPN

connection is Auto-disconnected. 0 means this connection is always on.

Active as default route: Normally used when the mode is set to *Dial-out. If this is selected,* all packets, including internet packets, will route through the VPN tunnel; If this function is enabled, the performance of your Internet connection may be degraded Click **Apply** after changing the settings.

L2TP over IPSec (L2TP/IPSec) VPN Connection

IPSec: Enable to enhance your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with during transmission. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means that the connection is a tunnel only, with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses a 56 bit encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses a 168 (56*3) bit encryption method.
- **AES:** Stands for Advanced Encryption Standards, it uses a 128 bit encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS, using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function provides better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This key is for Internet Key Exchange (IKE) protocol and is a string of between 4 and 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and it authenticates keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides of the connection (router or hosts).

Remote Host Name (Optional): Enter hostname of the remote VPN device. This is a tunnel identifier and should match the Remote VPN device hostname. If it matches the tunnel will be connected; otherwise, it will be dropped.

Caution: This is only when the router acts as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter the hostname of the Local VPN device that establishes the VPN tunnel. By default, the Router's default Hostname is **home.gateway.**

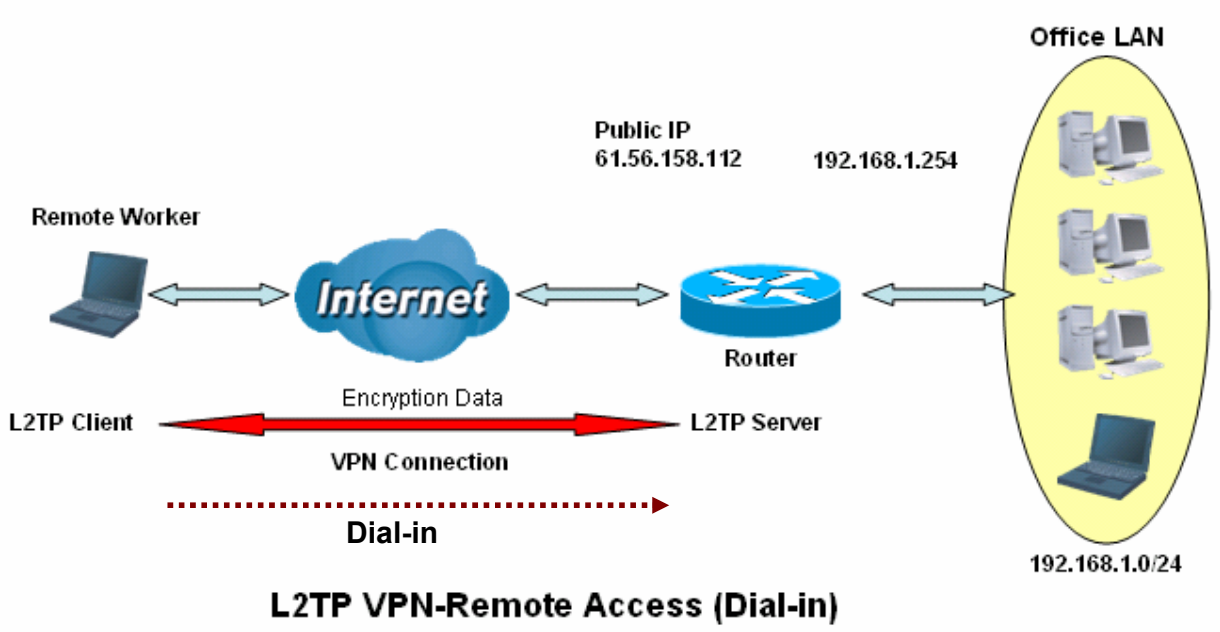
Tunnel Authentication: This enables the router to authenticate both the L2TP remote client and L2TP host. This is only valid when the L2TP remote client supports this feature.

Secret: The secure password length should be 16 characters (This may include numbers and/or characters.)

Click **Apply** after changing settings.

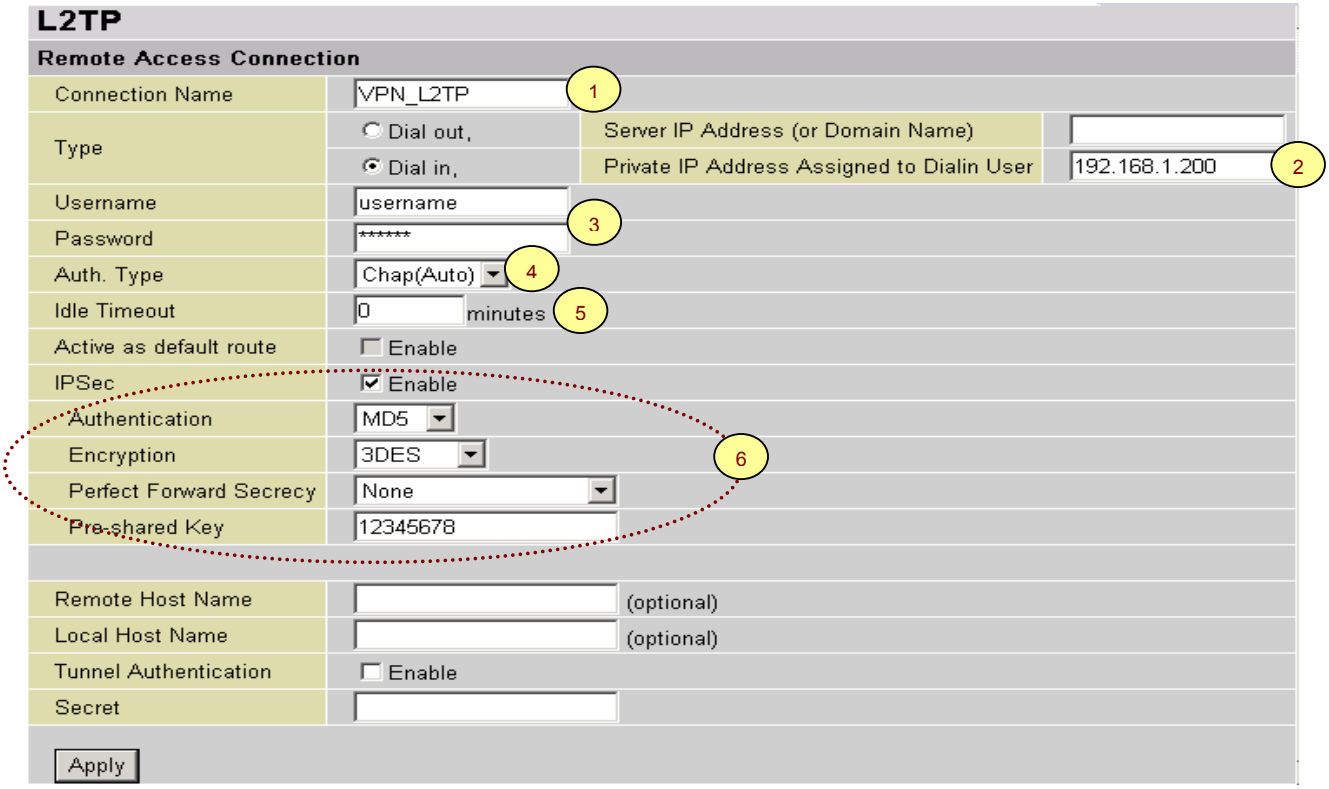
Example: Configuring a L2TP VPN - Remote Access Dial-in Connection

A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office and is connected to a couple of PCs and Servers.



Configuring L2TP VPN in the Office

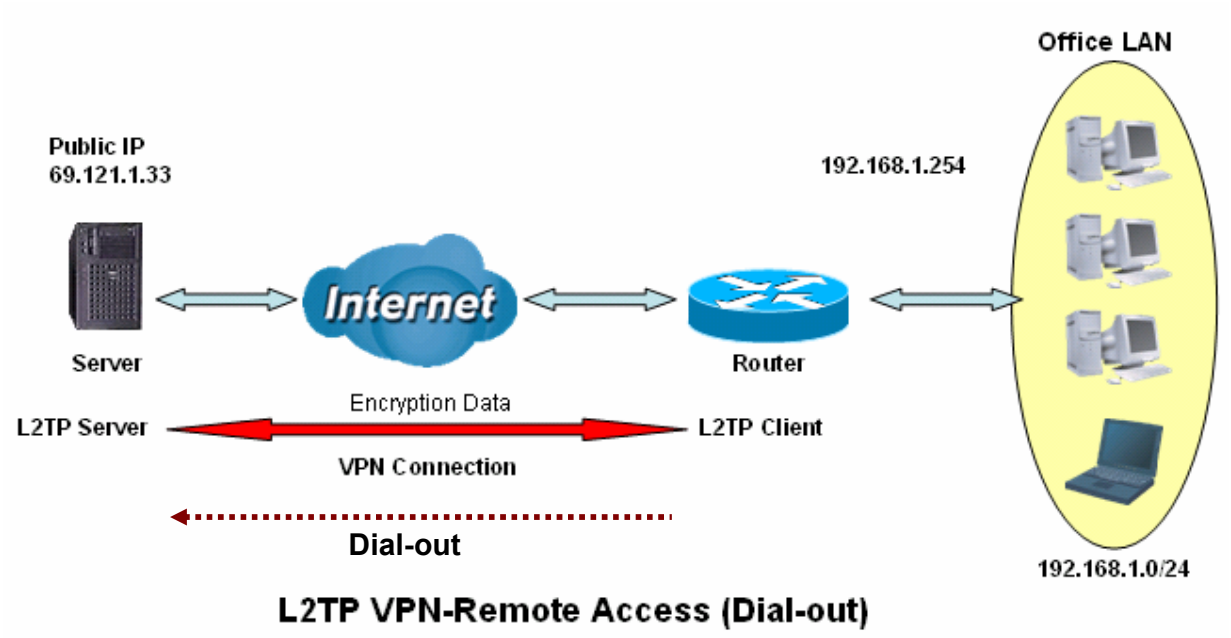
The LAN IP address 192.168.1.200 will be assigned to the remote computer (client). Please make sure this IP is not used on the Office LAN.



Item	Function		Description
1	Connection Name	VPN_L2TP	Given name of the L2TP connection
2	Dial in		select **Dial in**
	Private IP Address Assigned to Dialing User	192.168.1.200	The IP address to be assigned to the remote client
3	Username	username	The username & password that the remote client will use to authenticate the connection.
	Password	123456	
4	Auth.Type	Chap(Auto)	In most of the cases you should keep the default value of authentication type for maximum connection security.
5	Idle Timeout	0	The connection will be disconnected when there is no traffic over it for this predefined period of time. If Idle time is set to 0, it means that the connection will never time out.
6	IPSec		Select **Enable** to enhance your L2TP VPN security.
	Authentication	MD5	Both sides of the tunnel should use the same settings for these options.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring a Remote Access L2TP VPN Dial-out Connection

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office and is connected to a couple of computers and Servers.



L2TP VPN-Remote Access (Dial-out)

Configuring the L2TP VPN in the Office

L2TP

Remote Access Connection

Connection Name	VPN_L2TP (1)		
Type	(•) Dial out,	Server IP Address (or Domain Name)	69.121.1.33 (2)
	( ) Dial in,	Private IP Address Assigned to Dialin User	
Username	username (3)		
Password	******		
Auth. Type	Chap(Auto) (4)		
Idle Timeout	0 minutes (5)		
Active as default route	[ ] Enable		
IPSec	[x] Enable		
Authentication	MD5		
Encryption	3DES (6)		
Perfect Forward Secrecy	None		
Pre-shared Key	12345678		
Remote Host Name	(optional)		
Local Host Name	(optional)		
Tunnel Authentication	[ ] Enable		
Secret			

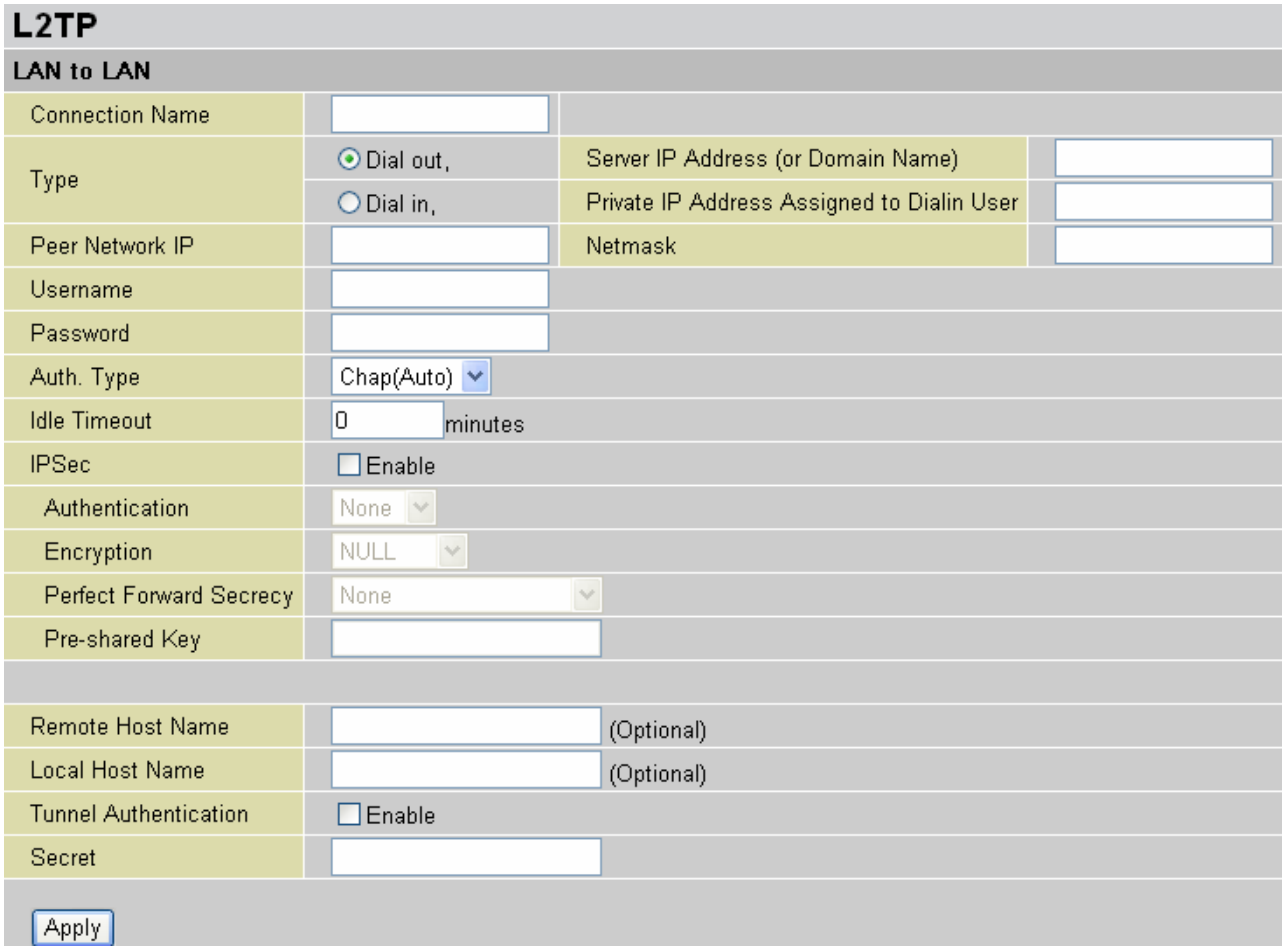
Apply

Item	Function		Description
1	Connection Name	VPN_L2TP	Given name of the L2TP connection
2	Dial out		select **Dial out**
	Server IP Address (or Hostname)	69.121.1.33	The Dialed server's IP address.
3	Username	username	The username & password that is required to connect to the VPN server.
	Password	123456	
4	Auth.Type	Chap(Auto)	Keep this default value in most of the cases.
5	Idle Timeout	0	The connection will be disconnected when there is no traffic over it for this predefined period of time. If Idle time is set to 0, it means that the connection will never time out.
6	IPSec		Select **Enable** to enhance your L2TP VPN security..
	Authentication	MD5	Both sides of the tunnel should use the same settings for these options
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring your Router to Dial-in to the Server

Currently, Microsoft Windows operation system does not support L2TP incoming service. Additional software may be required to set up your L2TP incoming service.

L2TP Connection - LAN to LAN



L2TP VPN Connection

Connection Name: A User-define description of the connection.

Type: Select **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), Select **Dial In** if you want your router to operate as a VPN server.

- When configuring your router to establish a connection to a remote LAN, enter the remote **Server IP Address (or Hostname)** that you wish to connection to.
- When configuring your router as a server, to accept incoming connections, enter the **Private IP Address Assigned to Dial in User**.

Peer Network IP: Enter the Peer network's IP address.

Netmask: Enter the subnet mask of the peer network, based on the Peer Network IP setting.

Username: If you set your router to act as a Dial-Out user (client), enter the username provided by your Host (the user name to connect to the VPN server). If you are a Dial-In user (server), enter a username that clients will need to use to connect to the router.

Password: If you set your router to act as a Dial-Out user (client), enter the password provided by your Host (the user name to connect to the VPN server). If you are a Dial-In user (server), enter a password that clients will need to use to connect to the router.

PPP Authentication Type: Default is **Auto.** Use this setting if you want the router to determine which authentication type to use. You can manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client) If the router is acting as a server enter the authentication type you want clients connecting to you to use. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Idle Time: When there is no activity on the connection for this pre-determined Idle time, the VPN connection is Auto-disconneced. 0 means this connection is always on.

Click **Apply** after changing settings.

L2TP over IPSec (L2TP/IPSec) VPN Connection

IPSec: Enable this setting to enhance your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with during transmission. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select your encryption method choice from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE means that the connection is a tunnel only, with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, and uses a 56 bit encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, and uses a 168 (56*3) bit encryption method.
- **AES:** Stands for Advanced Encryption Standards, and uses a 128 bit encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS, using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function provides better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups

Pre-shared Key: This key is for Internet Key Exchange (IKE) protocol and is a string of between 4 and 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and it authenticates keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides of the connection (router or hosts).

Remote Host Name (Optional): Enter hostname of the remote VPN device. This is a tunnel identifier and should match the Remote VPN device hostname. If it matches the tunnel will be connected; otherwise, it will be dropped.

Caution: This setting is only for when the router functions as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter the hostname of the Local VPN device that establishes the VPN tunnel. By default, the Router's default Hostname is **home.gateway.**

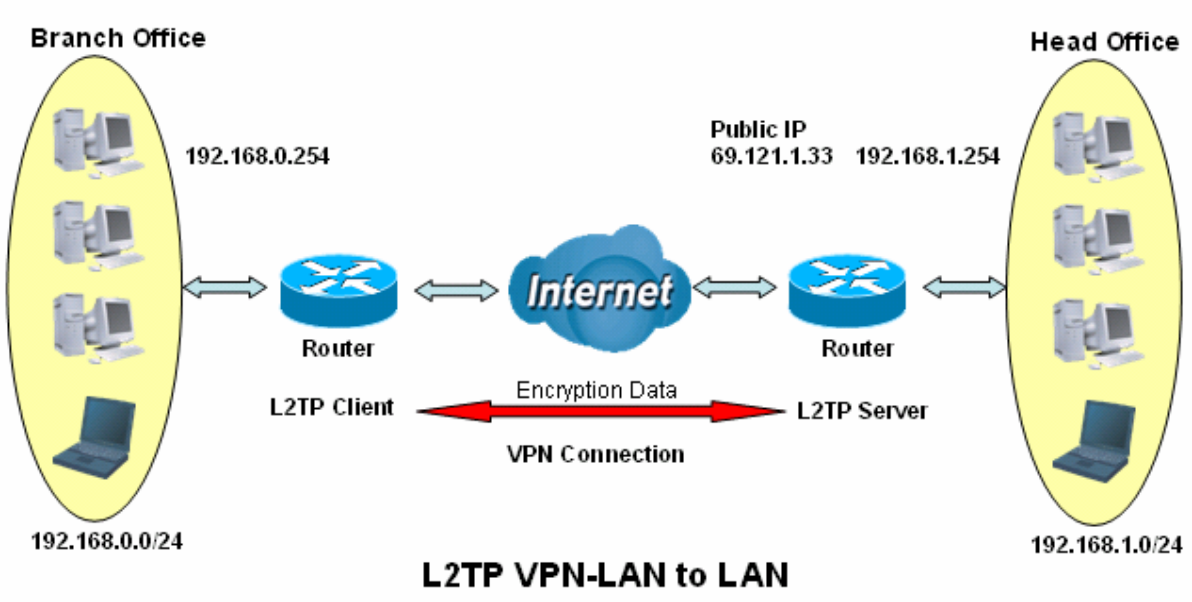
Tunnel Authentication: This enables the router to authenticate both the L2TP remote client and L2TP host. This is only valid when the L2TP remote client supports this feature..

Secret: The secure password length should be 16 characters (This may include numbers and/or characters.)

Click **Apply** after changing settings.

Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office, connecting the two private networks over the Internet. The routers are installed in both the head office and branch office.



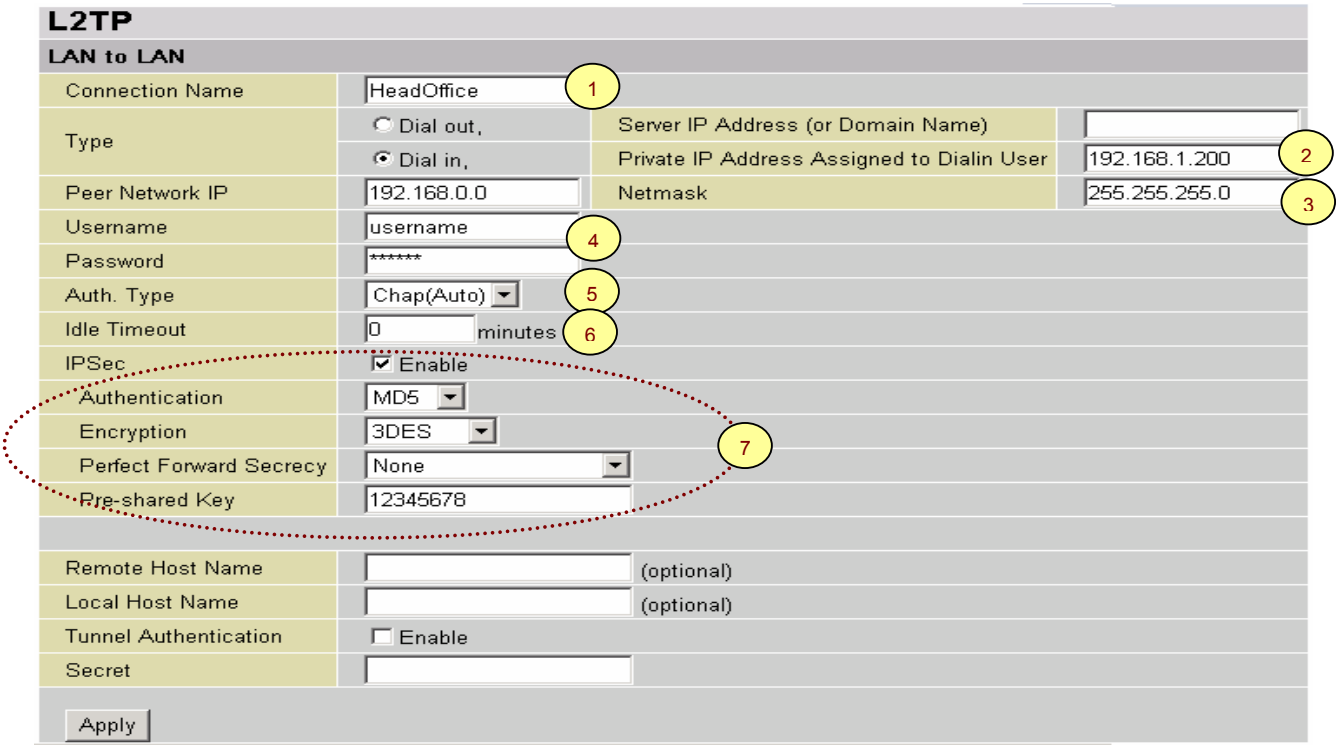
Attention

Both LAN networks **MUST be on different subnets** when using the LAN to LAN application.

The settings of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set on both routers.

Configuring L2TP VPN in the Head Office

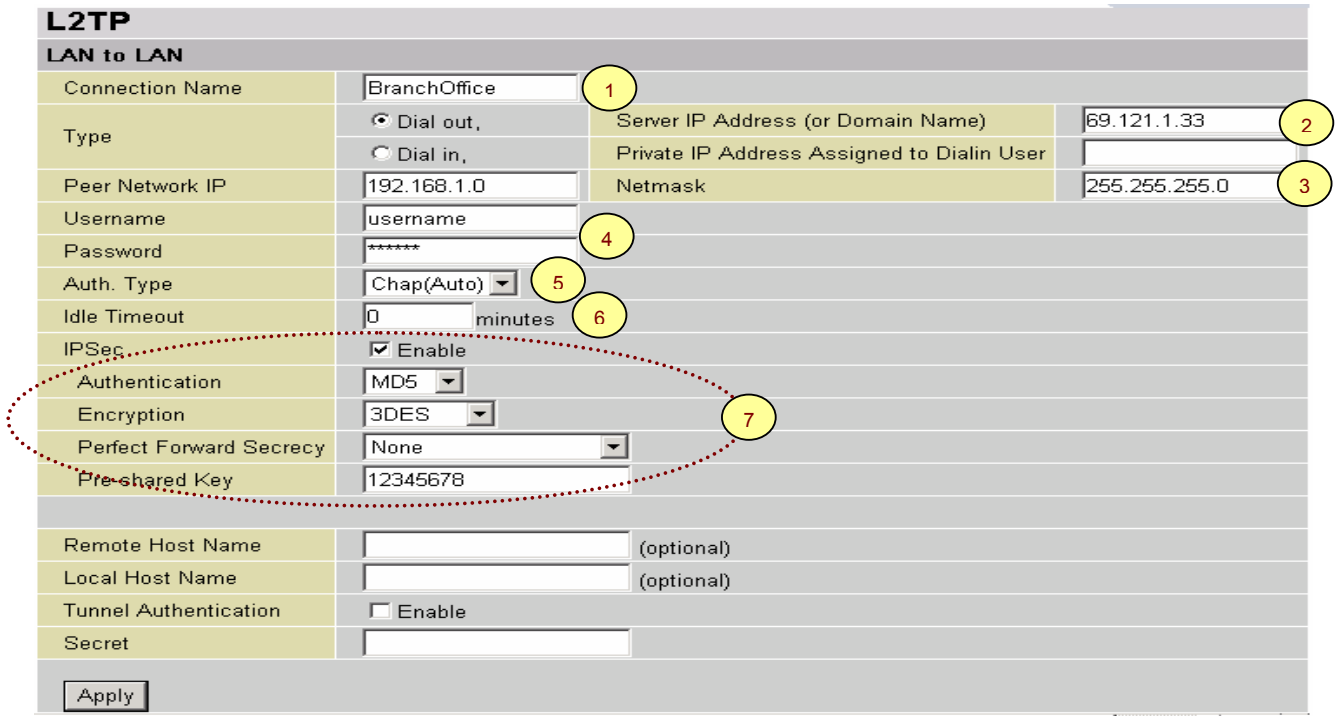
The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Connection Name	HeadOffice	Given name of the L2TP connection
2	Dial in		select **Dial** in
	Private IP Address Assigned to Dialing User	192.168.1.200	The IP address that will get assigned to branch offices network.
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	username	username & password that are used to authenticate the branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep these settings set to the default values in most cases.
6	Idle Timeout	0	The connection will be disconnected when there is no traffic over it for this predefined period of time. If Idle time is set to 0, it means that the connection will never time out.
7	IPSec		Select **Enable** to enhance your L2TP VPN security..
	Authentication	MD5	Both sides of the tunnel should use the same settings for these options.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Configuring L2TP VPN in the Branch Office

The IP address 69.1.121.30 is the **Public IP** address of the router located in head office. If you registered a DDNS account, (please refer to the **DDNS** section of this manual), you can also use the DDNS domain name instead of the IP address to reach the router.



Item	Function		Description
1	Connection Name	BranchOffice	Given name of the L2TP connection
2	Dial out		select **Dial** out
	Server IP Address (or Hostname)	69.121.1.33	IP address of the head office router (WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	username	Username & password required to to authenticate the branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep these settings set to the default values in most cases..
6	Idle Timeout	0	The connection will be disconnected when there is no traffic over it for this predefined period of time. If Idle time is set to 0, it means that the connection will never time out.
7	IPSec		Select **Enable** to enhance your L2TP VPN security...
	Authentication	MD5	Both sides of the tunnel should use the same settings for these options.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

VoIP - Voice over Internet Protocol

The VoIP functionality enables telephone calls to be placed through your existing Internet connection instead of going through the PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for long distance telephone calls, but also allows toll-quality voice calls to be placed over the Internet.

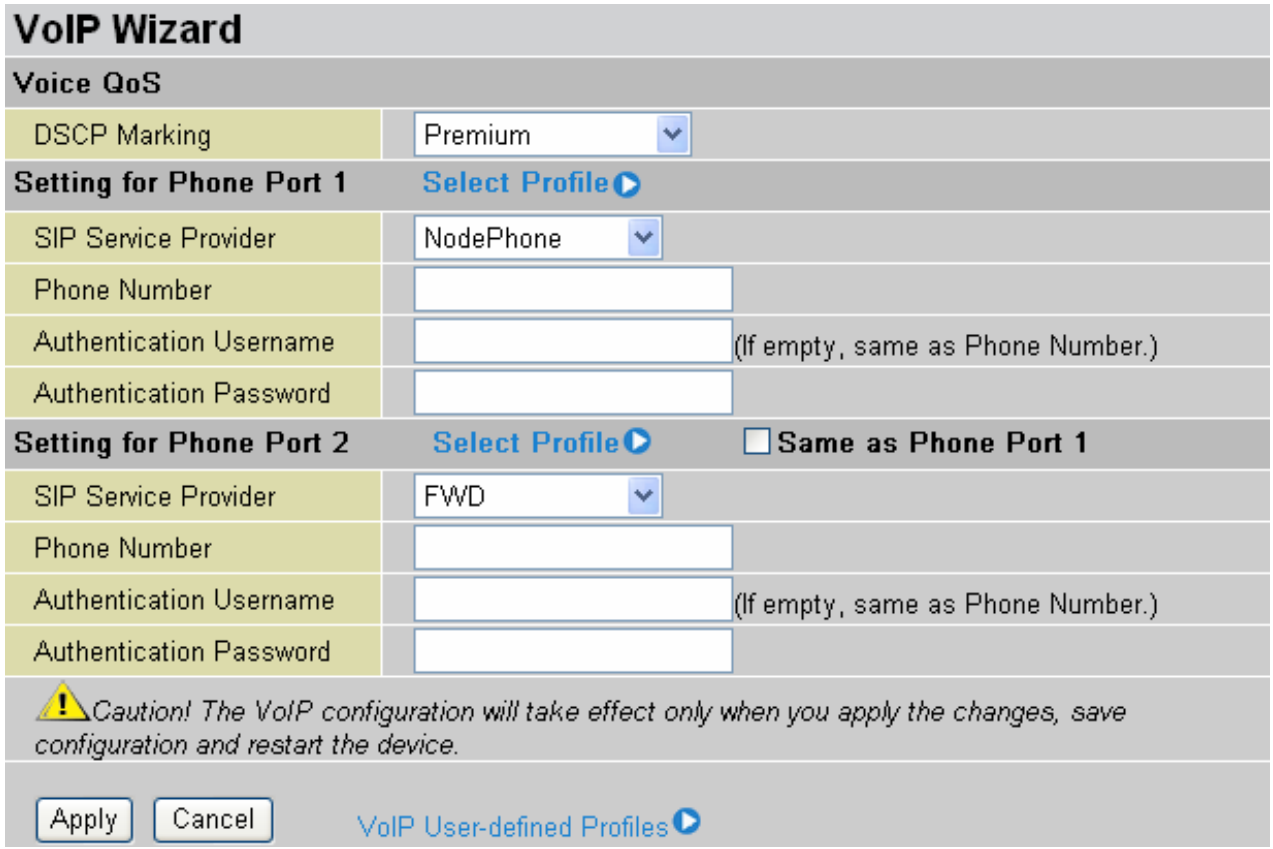
Attention

After completing your VoIP configuration, remember to apply the changes, SAVE CONFIG and restart to activate your VoIP functionality.

Here are the items within the **VoIP** section: **Wizard**, **General Settings**, **Phone Port, PSTN Dial Plan, VoIP Dial Plan** and **Ring &Tone**.

Wizard

This section provides an easy setup process for your VoIP service. Phone port 1 and 2 can be registered to different SIP Service Providers.



Voice QoS

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router on the backbone network, based on the DSCP value.

Note: To make use of this functionality, ensure that all of the routers in the backbones network have the capability of executing and checking DSCP through-out the entire QoS network.

Setting for Phone Port 1

SIP Service Provider: This section allows you to select your service provider. When the selection is done, the parameters below are automatically displayed.

Select Profile: This allows you to select a desired VoIP provider whom is not already defined in the *SIP Service Provider list.* You may manually setup the SIP accounts by entering VoIP SIP information into a *User-defined Profile*. See below for details.

Phone Number: This is the registration ID of the user as listed in the VoIP SIP registrar

Authentication Username: If the username is same as the Phone Number, leave it blank. Otherwise, fill in the space with your username given by your VoIP provider.

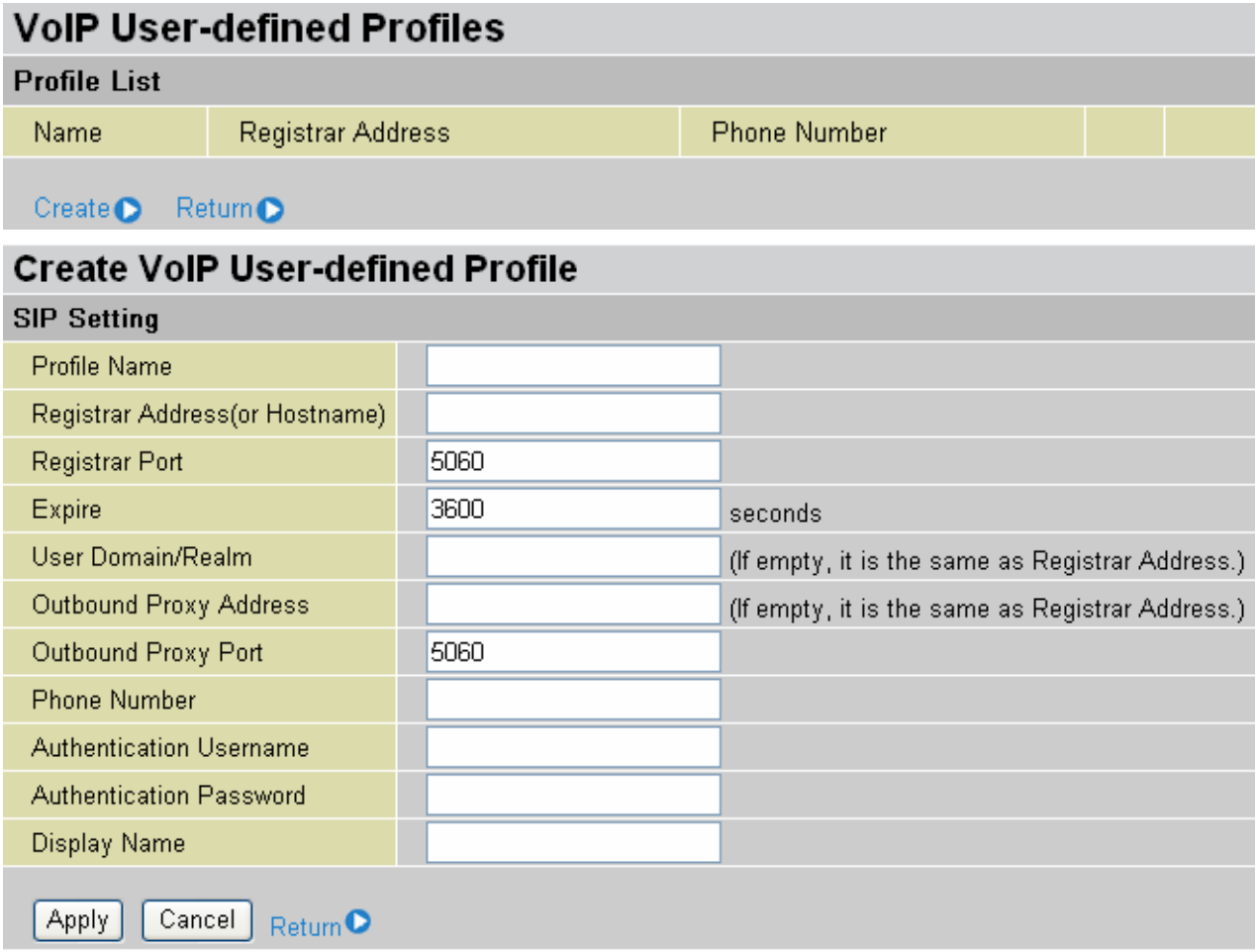
Authentication Password: This is the password used for authentication with the VoIP SIP registrar.

Setting for Phone Port 2

Select the **Same as Phone Port 1** box to set phone port 2 parameters to be identical to phone port 1. Otherwise, please refer to descriptions in “Setting for Phone Port 1”.

User-defined Profiles

Note: A maximum of 8 user defined profiles are allowed.



Profile Name: A user-defined name to identify the profile.

Registrar Address(or Hostname): Indicate the VoIP SIP registrar’s IP address.

Registrar Port: Specify the port on which the VoIP SIP registrar will listen for register requests from VoIP devices.

Expire: Expire time for the registration message sending.

User Domain/Realm: Set different domain names for the VoIP SIP proxy server.

Outbound Proxy Address: Indicate the VoIP SIP outbound proxy server IP address. This parameter is very useful when your VoIP device is behind NAT.

Outbound Proxy Port: Specify the port on which the VoIP SIP outbound proxy will listen for messages.

Phone Number: This is the registration ID of the user as listed in the VoIP SIP registrar.

Authentication Username: Same as Phone Number.

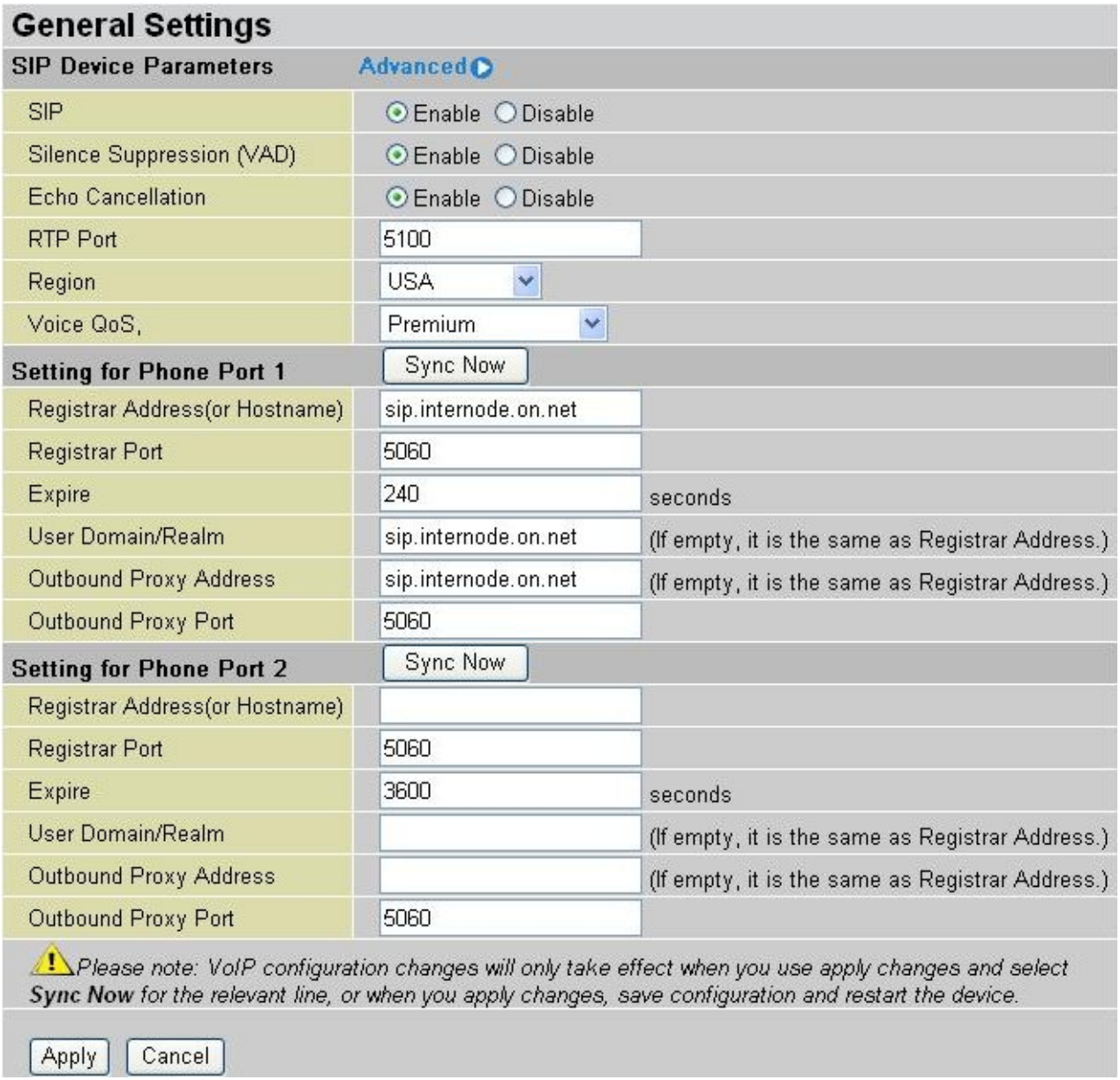
Authentication Password: This is the password used for authentication to the VoIP SIP registrar.

Confirm Password: Re-enter the password for confirmation.

Display Name: This is what will be displayed on a Caller ID system.

General Settings

This section contains the basic settings for the VoIP module from the selected provider in the Wizard section. If you do not provide correct information here, you will be unable to make calls over the Internet.



SIP Device Parameters

SIP: Select whether you wish to use SIP as VoIP call signaling protocol. The default setting is ***Disable.***

Silence Suppression (VAD): Voice Activation Detection (VAD) prevents the transmission of silence since it will unnecessarily consume your bandwidth. This function is also known as Silence Suppression, and it is a software application that ensures the bandwidth is used only when voice activity is activated. The default setting is ***Enable.***

Echo Cancellation: G.168 echo cancellation is an ITU-T standard. It is used for iremoving the echo while you are on the phone. If it is enabled, this will mean that you will not hear too much of your own voice on the phone while you talk. The default setting is ***Enable.***

RTP Port: Provide the base value for the media (RTP) ports. These ports are assigned to various

endpoints and the different call sessions that may exist within an end-point. (Range from 5100 to 65535, default value is 5100)

Region: This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically loaded.

Voice QoS,: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by backbone Routers, based on the DSCP value. See Table 4. The DSCP Mapping Table:

Note: To be sure that all the router(s) through-out the QoS network backbone have the capability of executing and checking the DSCP..

Setting for Phone Port 1

Registrar Address(or Hostname): Indicate the SIP registrar IP address.

Registrar Port: Specify the port on which the SIP registrar listens for register requests from VoIP devices.

Expire: Expiry time for registration message sending.

User Domain/Realm: Set a different domain name for the SIP proxy server.

Outbound Proxy Address: Indicate the SIP outbound proxy server IP address. This parameter is very useful when your VoIP device is behind NAT.

Outbound Proxy Port: Specify the port on which the VoIP SIP outbound proxy will listen for messages.

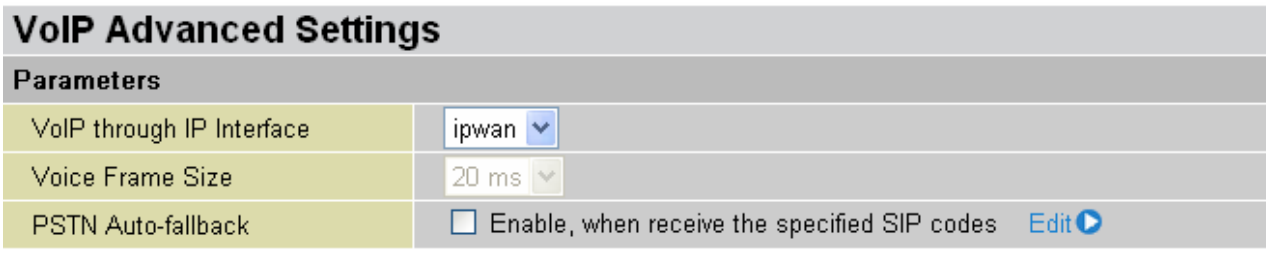
Setting for Phone Port 2

Please refer to the descriptions in “Setting for Phone Port 1”.

How to register with a SIP Server

1) On the Wizard Section page, select your VoIP Service Provider and provide information in the following fields: *Phone Number, Authentication Username* and *Authentication Password.*
2) On the Wizard Section page, click **Apply** to apply the settings.
3) On the General Settings page, make sure the general VoIP SIP information is correctly inserted.
4) On the General Settings page, click **Apply** to apply the settings.
5) On the General Settings page, click **Synch Now** to register the account(s) with your VoIP server.

Advanced – Parameters



VoIP through IP Interface: IP Interface decides where to send/receive the VoIP traffic. Options include: ipwan and iplan. An easy way to select the interface option is to check the location of the SIP server. If it is located somewhere on the Internet, then select **ipwan.** If the VoIP SIP server is on the local network then select **iplan.**

Voice Frame Size: Voice Frame size can be set anywhere between 10ms and 60ms. The function of Voice Frame Size is how many milliseconds the Voice packets will be queued for, before being sent out.

The ideal setting is to have the same frame size for both Caller and Receiver.

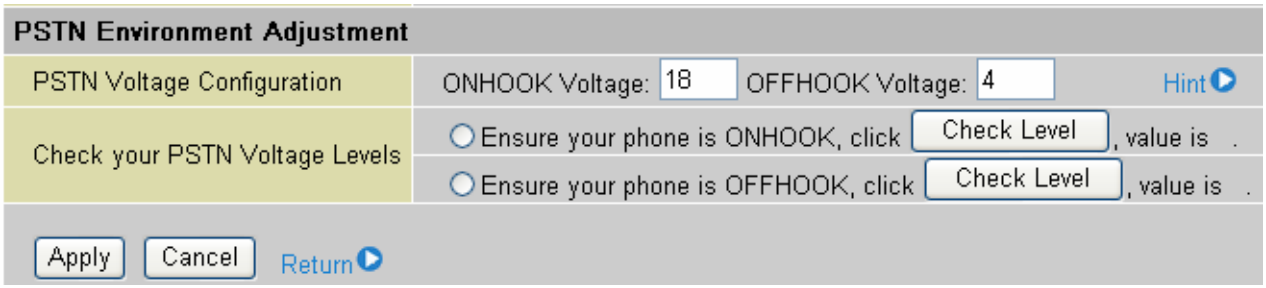
PSTN Auto-fallback: Whenever VoIP SIP response is an error code that matches the codes in the **Edit** section, the VoiP calls will automatically fall back to a PSTN.

Click **Edit** to add or remove codes. Be sure that the codes are separated by a comma**(,).**

For more information about SIP response codes, please click on Here to link to http://voip-info.org/wiki/view/sip+response+codes where you can find out the meaning of each error code.

Advanced – PSTN Environment Adjustment

The **PSTN Environment Adjustment** options will help you to adjust the on hook and off hook voltage detection values for your environment. The actual levels are determined by your environment including the number and type of telephones used. The default values provided are suitable for the South African PSTN network, and there should not be modified. If, however, you are connecting the line port to a PABX, and you experience problems with placing calls, then you may wish to modify these parameters.



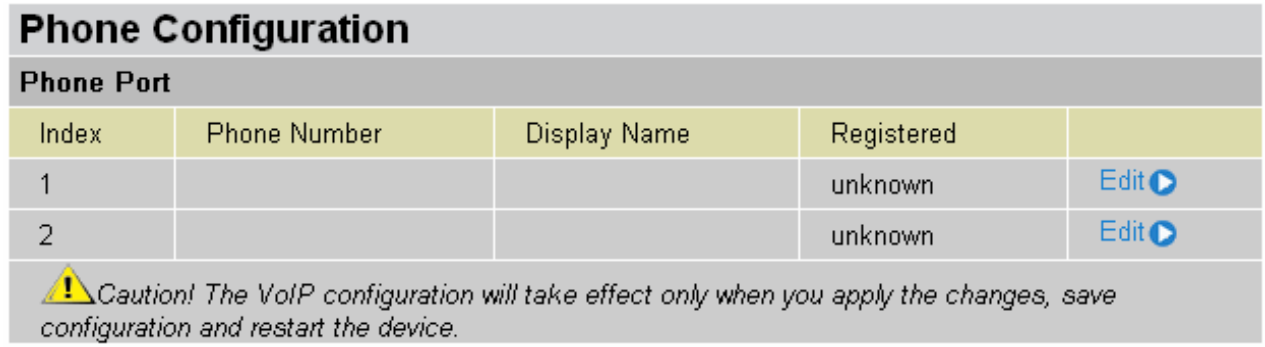
Note: ON HOOK means hung up.

To take your phone OFF HOOK, lift the receiver then press Hook/Flash until you hear your normal PSTN dial tone, not your VoIP dial tone. Wait several seconds and then press Check Level.

You should check the OFF HOOK value for each telephone you have connected to this device. Set the OFFHOOK voltage to the lowest setting registered for all your telephones, e.g. if your telephones return values of 4, 5 and 7 then you should set your OFFHOOK voltage to 4.
Note: The detected values will not automatically be set by the Check Level function; you must enter the lowest level detected after testing all your telephones.

Phone Port

This section displays status and allows you to edit the account information of your Phones. Click **Edit** to update your phone information.

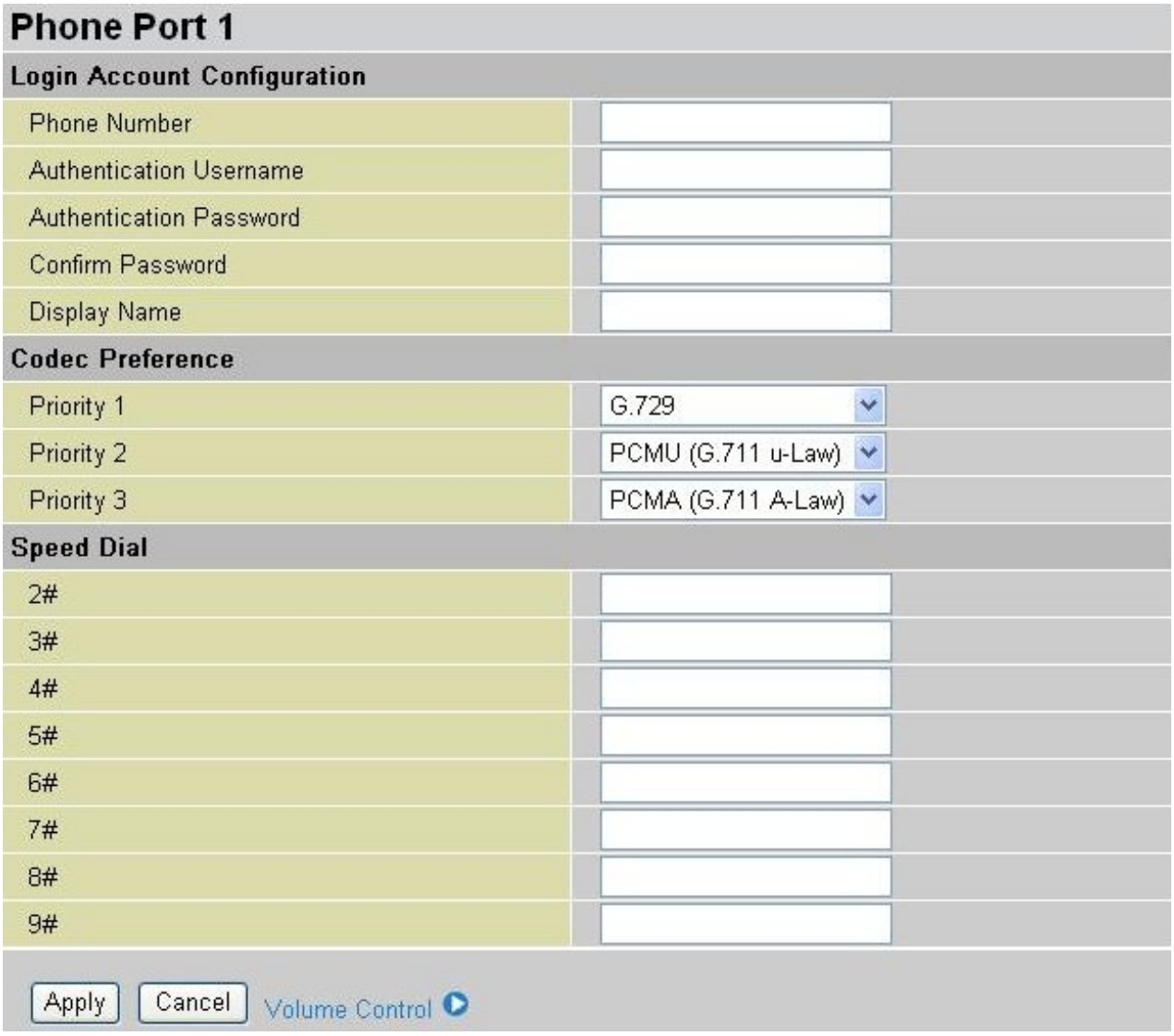


Phone Configuration

Phone Port

Index	Phone Number	Display Name	Registered	
1			unknown	Edit
2			unknown	Edit

Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.



Phone Port 1

Login Account Configuration	
Phone Number	
Authentication Username	
Authentication Password	
Confirm Password	
Display Name	
Codec Preference	
Priority 1	G.729
Priority 2	PCMU (G.711 u-Law)
Priority 3	PCMA (G.711 A-Law)
Speed Dial	
2#	
3#	
4#	
5#	
6#	
7#	
8#	
9#	

Apply Cancel Volume Control

Login Account Configuration

Phone Number: This parameter is the registration ID of the user as recorded in the VoIP SIP registrar.

Authentication Username: Same as Phone Number.

Authentication Password: This is the password used for authentication with the VoIP SIP registrar.

Confirm Password: Re-enter the password for confirmation.

Display Name: This is what will be shown when using the Caller ID function .

Codec Preference

A codec is a Coder-Decoder and is used for data signal conversion. The priority position sets the priority of each codec; Priority 1 is the top priority.

G.729: This type of codec encodes and decodes the voice information into a single packet which reduces the bandwidth consumption. 8kbps of bandwidth is needed.

G.711µ-LAW: This codec uses a basic non-compressed encoder and decoder technique. µ-LAW uses a pulse code modulation (PCM) encoder and decoder to convert voice into a 14-bit linear sample. 64kbps of bandwidth is needed.

G.711A-LAW: This codec uses a basic non-compressed encoding and decoding technique. µ-LAW uses a pulse code modulation (PCM) encoder and decoder to convert voice into a 13-bit linear sample. 64kbps of bandwidth is needed.

Non-used: This option is only available for Priority 2 and 3. It should be selected if no codec is to be used in these priority settings .

Note: In the example screen shown above, the codec priority is assigned in the order as G.729 > G.711µ-LAW > G.711A-LAW.

Speed Dial

The Speed Dial function is usefull for storing frequently used telephone numbers. You can press a number from 0 to 9 and the hash sign (#) on the phone keypad to call a speed dial number. For example, to phone a speed dial number listed under 9, press keypad **9** then **#**. Your router will automatically dial the number listed in entry 9.

For examples:

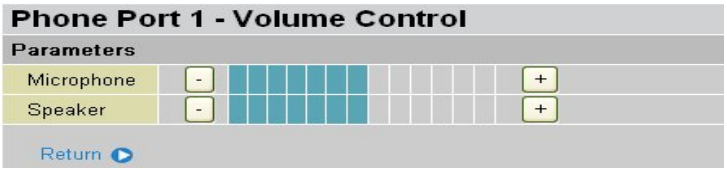
If your friend Tim gives you a SIP URL as sip: 89755@192.246.69.223 then you can fill in 89755@192.246.69.223. as number 1 speed dial.

If your friend Felix gives you a SIP URL as sip: felix@iptel.org then you can fill in felix@iptel.org. as number 2 speed dial.

If your friend Greg gives you an IP address "192.246.56.56" only, then you can fill in “192.246.56.56”.

In some cases, when a user makes use of DDNS, you will have to fill in their domain name as well.

Volume Control



The Volume control setting helps you to adjust the voice level of the telephone to the most comfortable listening level.

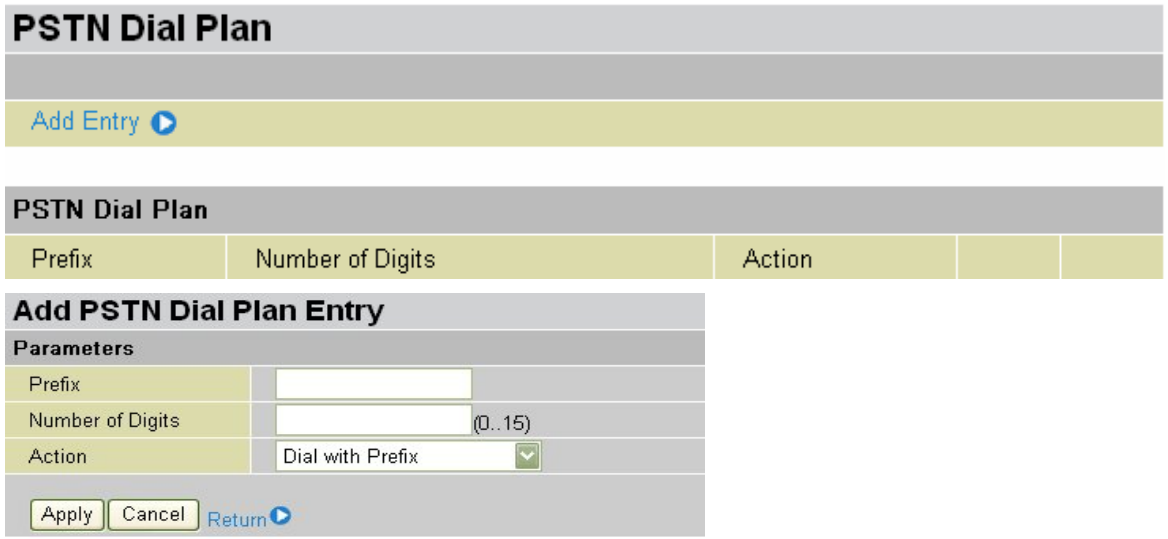
Press “**-**“, the minus sign, to reduce either the microphone and/or the speaker’s volume of your telephone.

Press “**+**“, the plus sign, to increase either the microphone and/or the speaker’s volume of your telephone.

PSTN Dial Plan

This section enables you to configure "VoIP with PSTN switching" on your system. You can define a range of dial plans to select which calls are routed over VoIP and which are routed over the PSTN line. Prefix numbers are the essential key to distinguish between VoIP and Regular (PSTN) phone calls. If the actual numbers dialed matches the prefix number defined in this dial plan, the dialed number will be routed to the PSTN to make a regular call. Otherwise, the number will be routed over the VoIP network.

Reminder! *In order to utilize this feature, you must have registered and connected to your SIP Server first.*



Prefix: Specify number(s) for switching to a PSTN call.

Number of Digits: Specify the total number of digits that you wish to dial out. Maximum digit number is 15.

Action: Specify a dialing method that you wish to use when making PSTN call(s).

- **Dial with Prefix:** The complete number that you have dialed will be dialed on the PSTN (including prefix)

Note: The actual number of valid digits dialed must match the number in the **Number of Digits** field.

- **Dial without Prefix:** The number that you have dialed will be dialed on the PSTN after the prefix has been removed from it (excluding prefix).

Note: The actual number of valid digits dialed must match the number in the **Number of Digits** field

- **Dial at Timeout:** The complete number that you have dialed will be dialed on the PSTN (including prefix) once a certain time has elapsed since the last digit was dialed.

Note: The actual number of valid digits dialed must NOT EXCEDE the number in the **Number of Digits** field.

- **Dial at Timeout no prefix:** The number that you have dialed will be dialed on the PSTN after the prefix has been removed, (excluding the prefix) once a certain time has elapsed since the last digit was dialed.

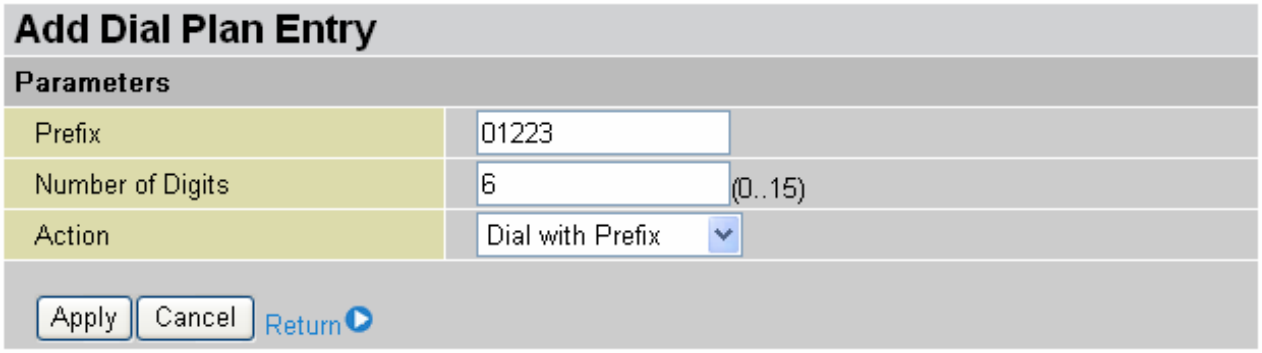
Note: **The actual number of valid digits dialed must NOT EXCEDE the number in the** Number of Digits **field**

Attention

Phone port 1 and 2 will automatically default to the PSTN line when:
- **The router is Powered Down**
- **Internet Service Fails**, i.e., lost of WAN IP Address/connection
- **The SIP option is disabled.** See the *VoIP General Setting* section.
- **Calls that are placed match the rule(s) defined in the *PSTN Dial Plan.***
- **The SIP service is not accessible.** This does not include when :
  - A User manually disables Registration.
  - A User inserts a wrong authentication username and/or password.
  - A User dials a wrong SIP number, only and if, the *PSTN Auto-Fallback* function is not enabled. See *VoIP General Setting / Advanced* for information.

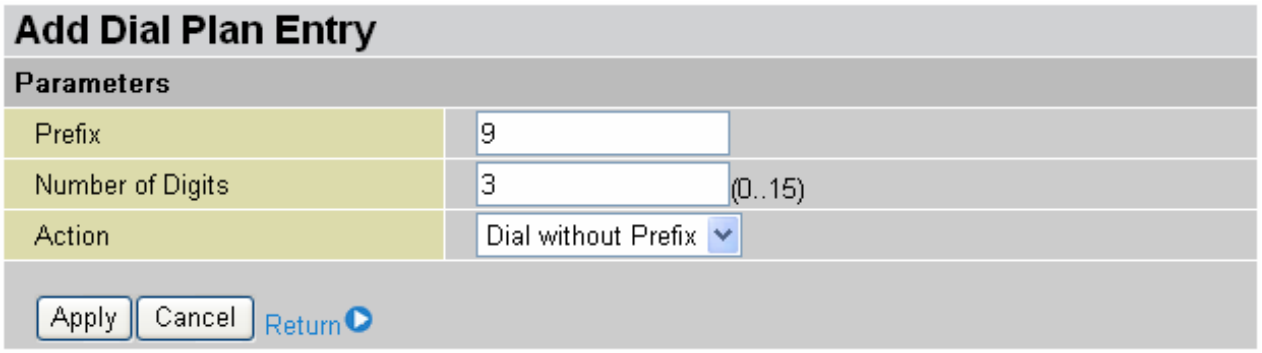
PSTN Dial Plan Examples:

1) Dial with Prefix



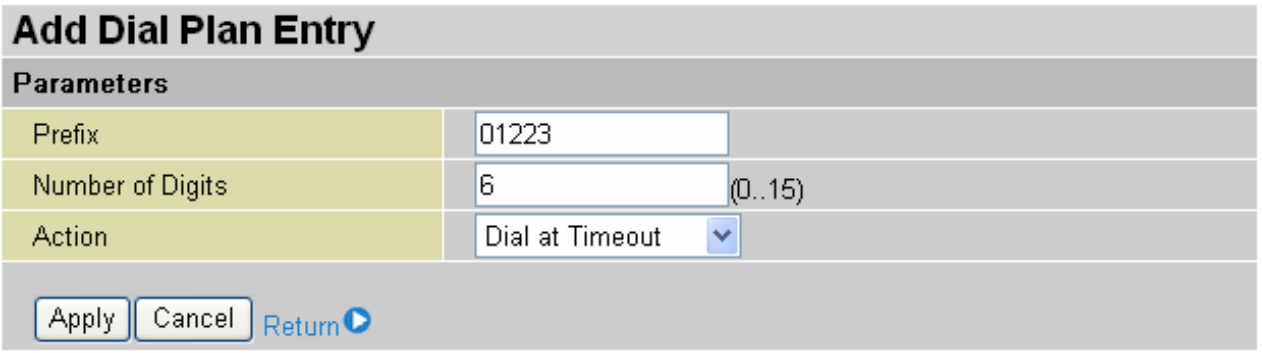
If you dial 01223 707070, the number 01223707070 will be dialed out via the FXO port, to make a regular (PSTN) phone call.

2) Dial without Prefix



If you dial 9102, the number 102 will be dialed out via the FXO port, to make a regular (PSTN) phone call.

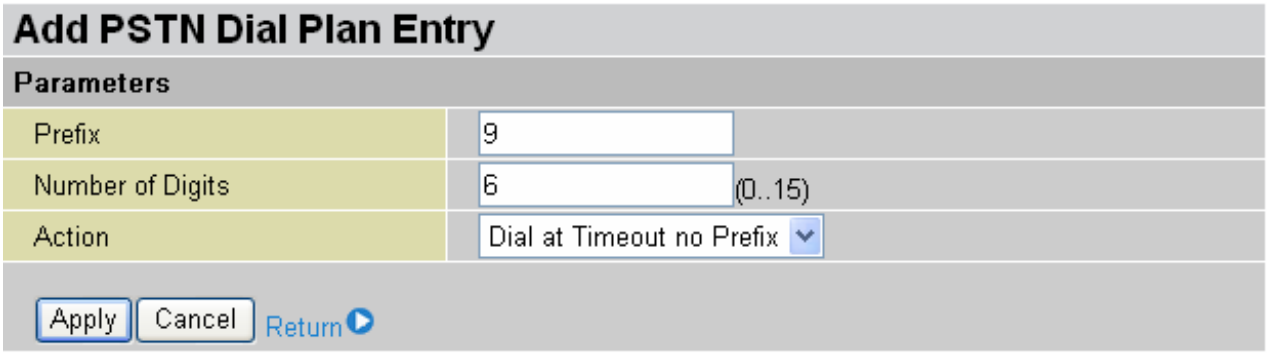
3) Dial at Timeout



If you only dial 01223 7070 and no more numbers, after the timeout occurs , 012237070 will be dialed to make a regular (PSTN) call via the FXO port.

Even though 7070 (only 4 digits) does not match the number of digits (6) defined in the Number of Digits field, 7070 is still a valid phone number since it has not exceed this Number.

4) Dial at Timeout no Prefix

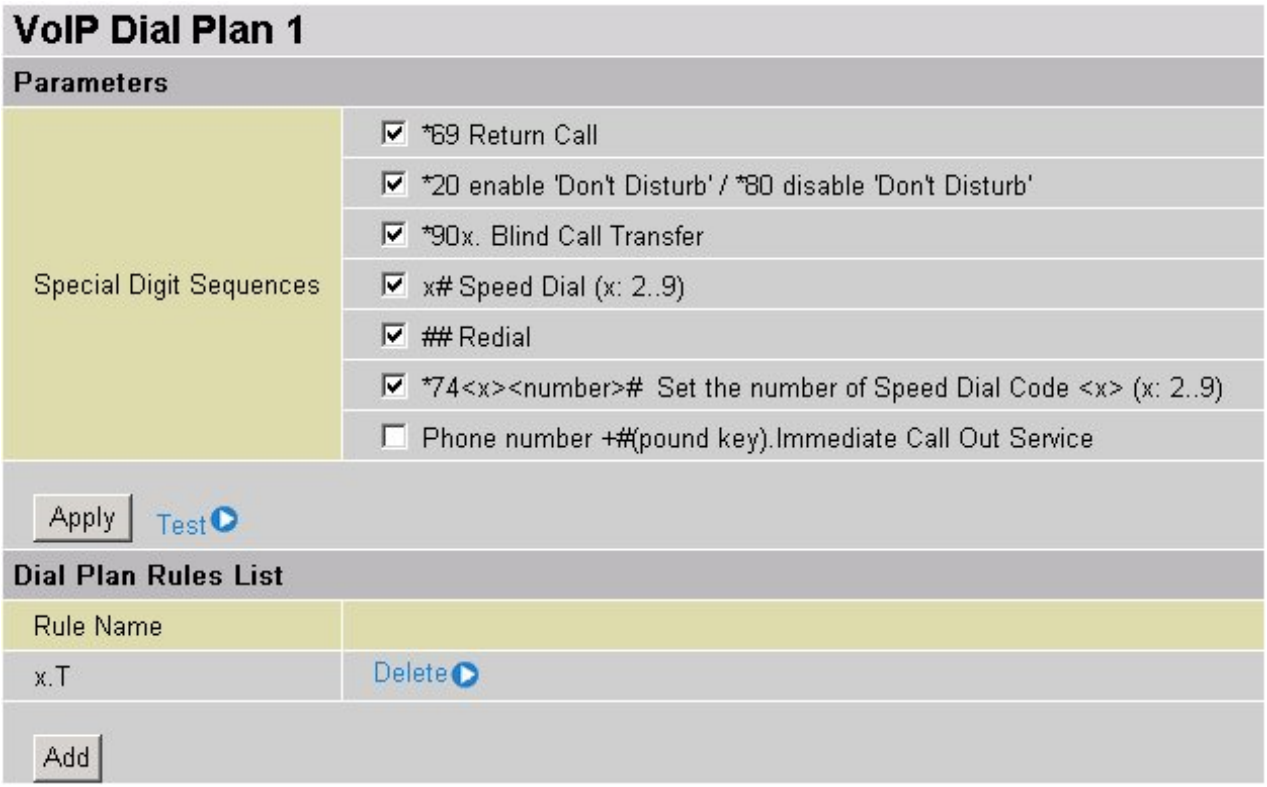


If you dial 97070 and no more numbers, after the timeout activates, 7070 will be dialed (without the prefix), to make a regular (PSTN) call via the FXO port.

Even though 7070 (only 4 digits) does not match the number of digits (6) defined in the Number of Digits field, 7070 is still a valid phone number since it has not exceed this Number.

VoIP Dial Plan

This section helps you to make a VoIP call as easily as a regular call. You no longer need to memorize a long dial string of numbers in order to make a VoIP call.



Parameters

A list of special dial features comes handy when you have a miss call or need to transfer a call to a third party. For details, please refer to the section **Special dial codes** below.

***69 (Return Call):** Dial *69 to return the last missed call. This is only available for VoIP call(s).

***20 (Turn Do Not Disturb on):** Dial *20 to turn the **Do Not Disturb** mode on. Your phone will not ring if someone calls.

***80 (Turn Do not Disturb off):** Dial *80 to turn the **Do Not Disturb** mode off. Your will ring when someone calls.

***90x (Blind Call Transfer):** Dial *90 + phone-number to transfer a call to a third party. This feature is enabled by default.

x# Speed Dial (x = 2..9): Refer to the **Phone Port** section in the Web GUI. Set up your Speed Dial phone book first before accessing the Speed Dial feature. This feature is enabled by default.

Redial: Press ## to redial the latest number you dialed. This feature is enabled by default.

***74<x><number>#:** Use your phone key pad to insert a phone number into the Speed Dial phone book. you can also update your Speed Dial phone numbers manually. Refer to the **Phone Port** section in the Web GUI for details.

Phone Number + #: This is the fast dial mode, and it will dial out a phone number immediately after the number is entered, without waiting.

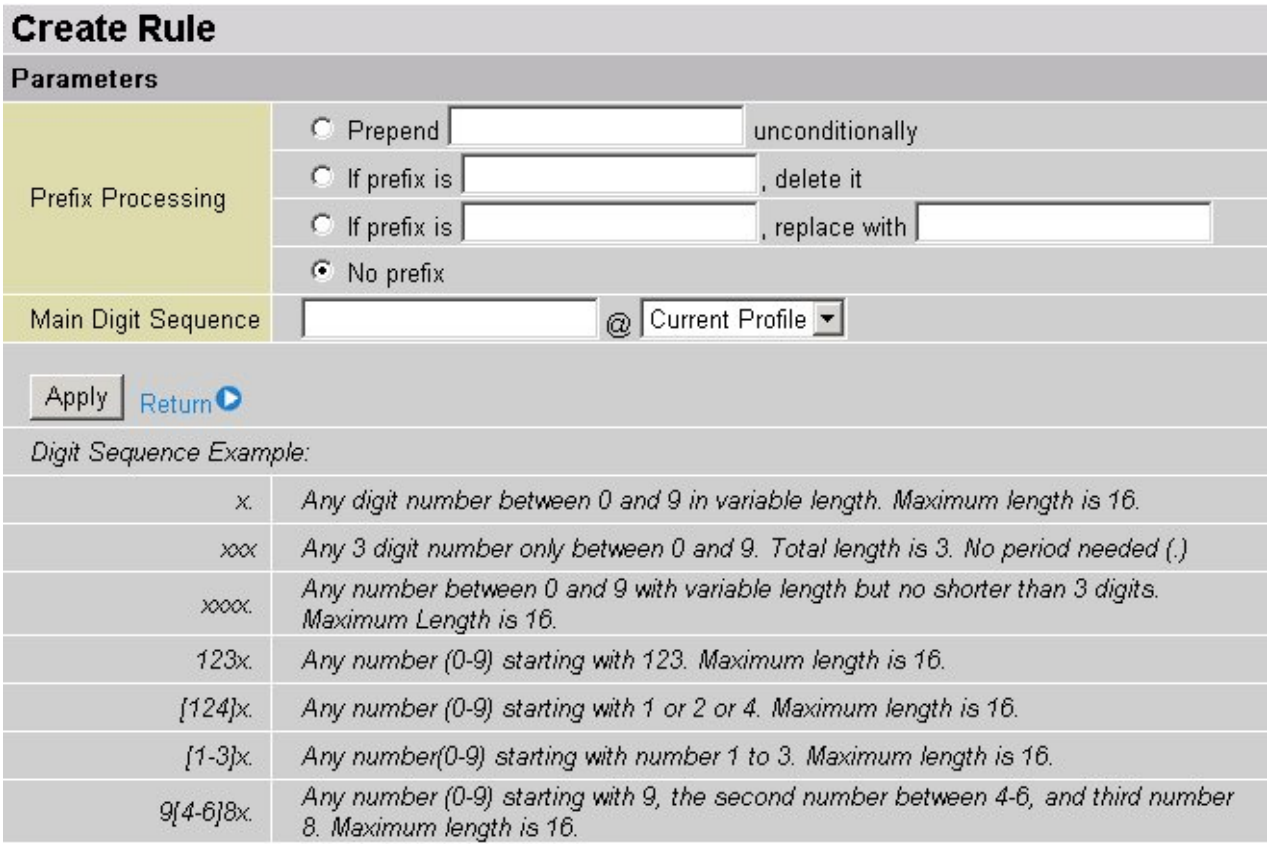
Note: Refer to Special Dial Code section in this Manual for more details.

Test: this function is a tool to help you identify that the call number is being properly processed prior to making an actual call.

Click **Apply** to apply the settings.

Dial Plan Rules List

Click **Add** to create and define VoIP dial-plan rule(s).


Create Rule
Parameters
Prefix Processing
Prepend unconditionally
If prefix is , delete it
If prefix is , replace with
No prefix
Main Digit Sequence
@ Current Profile
Apply
Return
Digit Sequence Example:
x. Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx. Any 3 digit number only between 0 and 9. Total length is 3. No period needed (.)
xxxx. Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum Length is 16.
123x. Any number (0-9) starting with 123. Maximum length is 16.
[124]x. Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[1-3]x. Any number(0-9) starting with number 1 to 3. Maximum length is 16.
9[4-6]8x. Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.

Prefix Processing:

Prepend xxx unconditionally: The entered number, xxx, is appended unconditionally to the front of the dialing number when making a call. This prefix can include any number and/or character such as **+**, ***, #**.

Note: For special services using +, *or #, you may need to check with your VoIP or Local Telephone Service Provider for information pertaining to correct usage.

If Prefix is xxx, delete it: If the prefix is the same as the specified number, xxx, it will be removed from the dialed number before making a call.

If Prefix is xxx, replace with: If the prefix is the same as the specified number, xxx, it will be appended to the front of the dialed number before making a call.

No prefix: No prefix is appended to the front of the dialing numbers. This is the default setting.

Main Digit Sequence: The call(s) can be dialed out via SIP, PSTN or ENUM.

x: Any numeric number between 0 and 9.

. (period): Repeat numeric number(s) between 0 and 9.

*** (asterisk sign): T**his is the normal character '*' found on a phones keypad. Please check if this is used by your VoIP Service Provider or Local Telephone Service Provider for special services.

 # (pound sign): This is the normal character '#' found on a phone keypad. Please check if this is used by your VoIP Service Provider or Local Telephone Service Provider for special services.

<@ Current Profile>: This Referes to your VoIP account as registered using the *VoIP Wizard* for Port 1 /

2.

<@ PSTN>: This referes to making calls via the PSTN line.

<@ENUM>: This referes to making a VoIP SIP call, via an E.164 number ("ENUM"), to an ENUM callee. Electronic Number (ENUM) is a system that uses DNS (Domain Network System) based technology to map between a traditional phone number (PSTN) and an Internet address/ SIP URL. The ENUM number must be registered on a public ENUM site or with your VoIP Service Provider.

<@ SIPgateway>: This is used when using the *Intelligent Call Routing* feature. You will need to set up your SIP account on the **VoIP User-defined Profiles** link on the VoIP Wizard page. Go to the *VoIP Wizard* in this manual for more information.

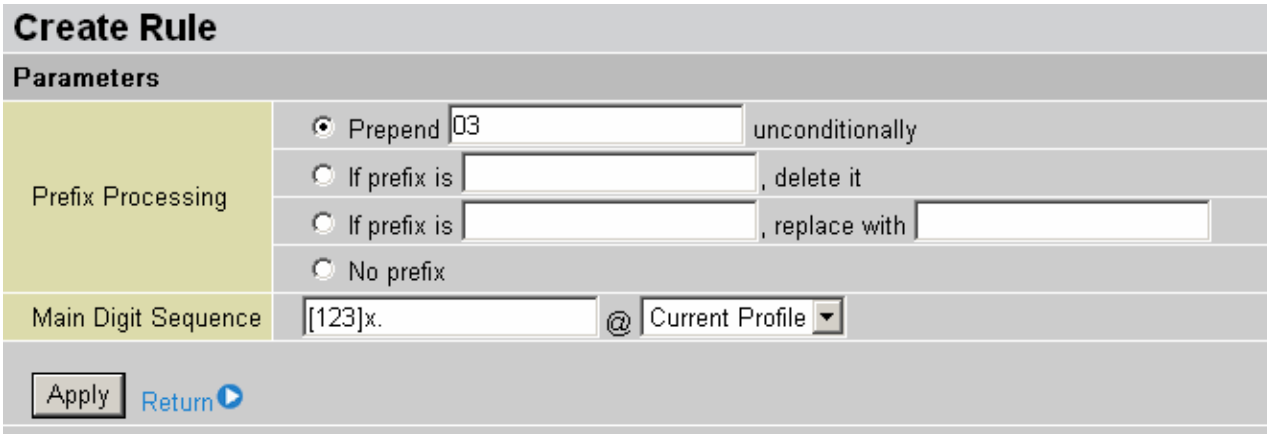
Dial-Plan Examples:	**Description**
x.	Any sequence of digits between 0 and 9. Maximum sequence length is 16.
xxx	Any 3 digit (between 0 and 9) number. Total sequence length is 3. Note: No period is needed (.)
xxxx.	Any sequence of digits (between 0 and 9) between 3 an 16 digets long .
123x.	Any number (0-9) starting with 123. Maximum length is 16.
[x…x]x. For example: [124]x.	Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[x-x]x. For example: [1-3]x.	Any number (0-9) starting with a number between 1 and 3. Maximum length is 16.
x[x-x]x. For example: 9[4-6]8x.	Any number (0-9) starting with 9, the second number being any number between 4-6, and the third number being 8. Maximum length is 16.
Special Dial Plan Examples:	**Description**
*xx*x.	Starting with an asterisk, then any two digit number, a '* sign', and any number of additional digits. Maximum length is 16.
*xx	Starting with an asterisk, then any two digit number between 00 and 99. Total length including the * is 3 digits. Note: No period is needed (.)
**xx*x.	Starting with two asterisks, then any two digit number, a '* sign' and any number of additional digits. Maximum length is 16..
#xx.	Starting with '# sign', followed by any number with a length of between 1 and 16 digits.
##xx*x.	Starting with '## sign' , and followed by any two digit number, a '* sign' and ending in any number with a maximum length of 16.

<@SIPgateway> / Intelligent Call Routing Example:

The VoIP Gateway let you use 3 VoIP/SIP providers at the same time. Each provider has different prices for different type of calls so you can set you router make the best use of these different tariffs. Here are some examples of some rules you can set to make best use of each provider.

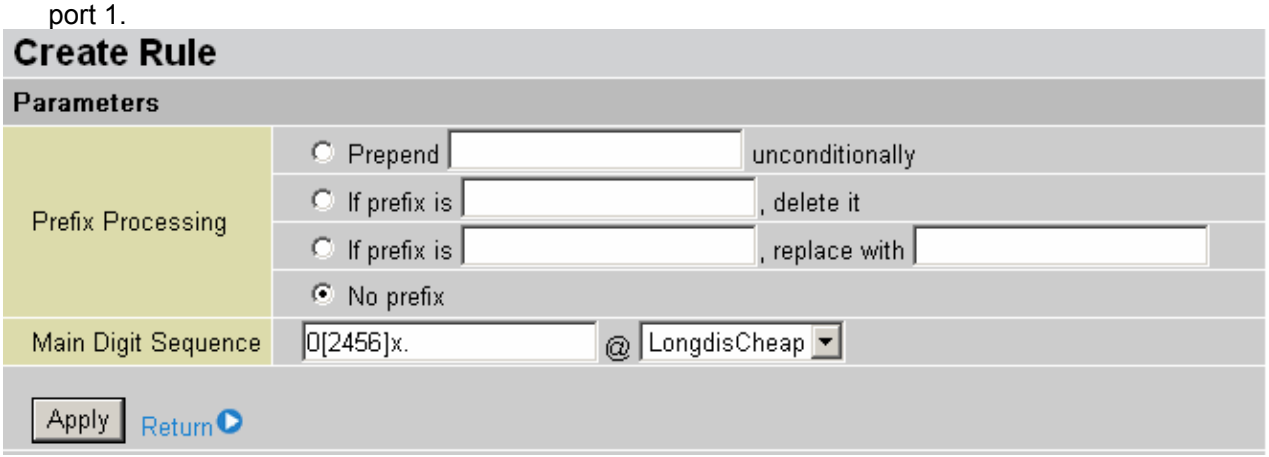
Imagine that there are 3 different VoIP providers by the name of *localcheap.com, Longdischeap.com and Mobilecheap.com*

1) Phone 1: For Local calls: I use *localcheap.com* who charge $0.01 per minute to all local calls. I set a dial rule, **<:03>[123]x.T**, on my phone port 1.



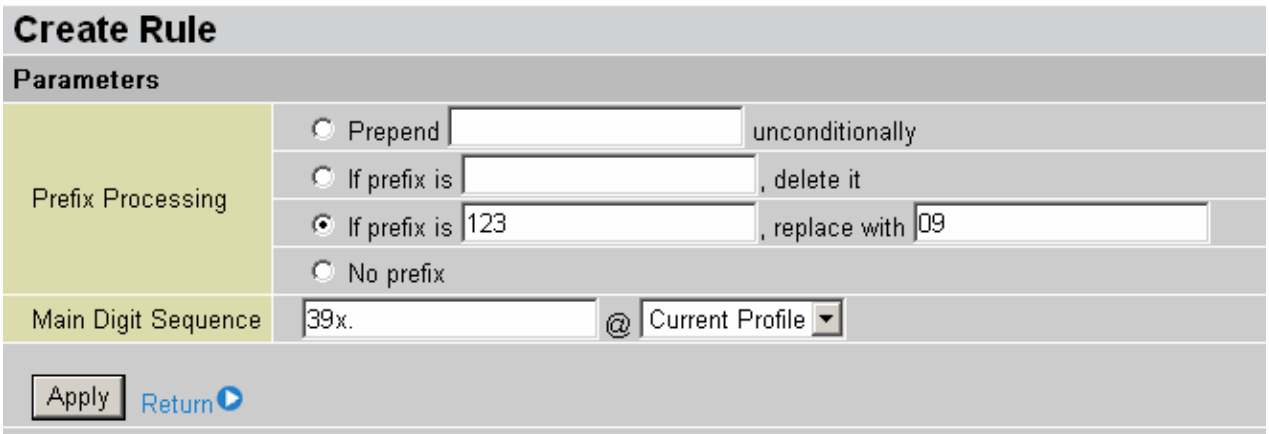
Localcheap.com is the default VoIP provider I set on phone port 1. When I dial any number starting with 1 or 2 or 3 , , 03 is always prepended in front of these number. If **2**3295 is dialed, 03-2-32935 is the actual phone number dialed using localcheap.com as a provider.

2) Phone 1: For International calls: I use *longdischeap.com* who charge $0.05 per minute for all International long distance calls. I set a dial rule, **0[2456]x.T<@Long_dist_Cheap>**, on my phone port 1.



Longislcheap.com is one of the VoIP providers I set in the User-defined profile. No prefix is attached to the dialed number when I dial any number beginning with 0 , followed by 2, 4, 5 or 6 and then the rest of the phone number. If **02**016148513295 is dialed, 0-2-016148513295 is the actual phone number dialed using longdischeap.com as a provider.

3) Phone 2: For Mobile calls, I use *mobilecheap.com* who charge $0.25 per minute for all local mobile calls. I set a dial rule, **<123:09>39x.T**, on my phone port 2.



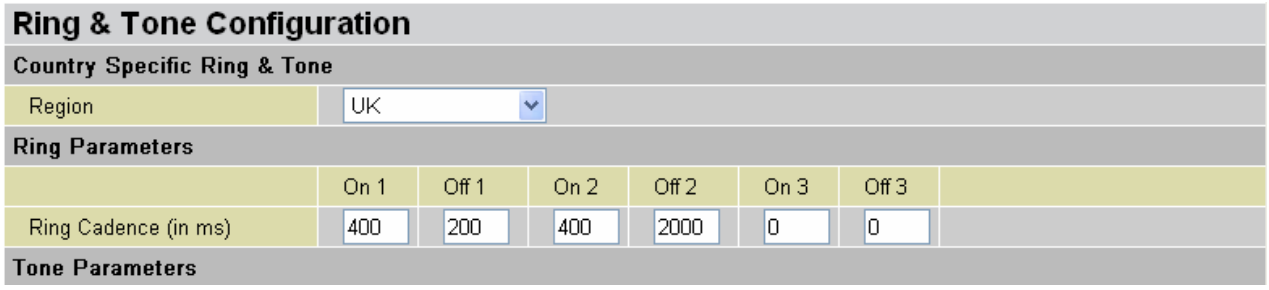
Mobilecheap.com is the default VoIP provider I set on phone port 2. When I call out 123-39-45678 for a

mobile call, 123 is replaced with 09 and 09-39-45678 is the actual phone number dialed using Mobilecheap.com as a provider.

The Intelligent Call Gateway not only saves time when changing VoIP settings to different providers so as to ensure a call gets routed using a specific gateway automatically, but it allows you to take advantage of different call rate.

Ring & Tone

This section allows advanced users to change the parameters for the various phone tones. (dialtone, busy tone, answer tone and etc.)The default settings are the same as the South African PSTN, but advanced users are welcome to customize these values to suit their requirements.



Country Specific Ring & Tone

Region: Select the country where you are located from the drop-down list,. This VoIP router provides default parameter of ring tones according to different countries. The ring-tone parameters are automatically displayed after entering a specific country. If your country is not in the list, or you wish to have a customised ring tone, you may manually create ring-tone parameters.

Ring Parameters

Ring Cadence (in ms): Ring cadence is defined by the following fields, Frequency: On Time1, Off Time1, On Time2, Off Time2 and On Time3, Off Time3. Frequency is specified in Hertz. Time is given in milliseconds.

Tone Parameters

You may need to check with your local telephone service provider for such information. Also, it is recommended that this option be configured by an advanced user only , unless you are instructed to do so.

Click **Apply** to apply the settings.

Special Dial Codes

The following table lists the special dial codes that are built into the router:

Option	Description
Flash-hook	Switch to PSTN line Note: This is a quick press of the hook switch. On most phones, a button is provided which provides Flash-hook functionality. The button is marked "FLASH","RECALL" or sometimes “R”
***69**	Return the last missed call (for SIP service only) Note: Entering this on a phone will call the last number that dialed the phone. For example A makes a call to B, but hangs up before B answers. If B enters *69, A will be called back .
##	Last dialed number redial function
***20**	Turn the Do Not Disturb mode on This mode enables a “Do Not Disturb” feature on a phone, such that any phone which calls it will receive an engaged tone and the called phone will not ring. For example, B enters *20 and hangs up. A makes a call to B, but receives the engaged tone. Phone B does not ring.
***80**	Set the Do Not Disturb mode off
***74<x><number>#**	Set the number for Speed dial code ‘x’, where ‘x’ is a number between 2 and 9. Note: <x> is a number between 2 and 9, and <number> is the number to dial. To dial a speed dial number from a phone connected to the VoIP Router , dial : **<x>#**, where **<x>** is a number between 2 and 9. These settings will affect your setting on the Speed Dial page of the WEB GUI.
***90<phone-number>**	This is how to make a **Blind Call Transfer**. With this function, the specified <phone-number> is the number that you wish to transfer the call to. This function is for a SIP service only. Note: You use **Blind Call Transfer** when you have a call in progress (incoming or outgoing) and decide you wish to transfer the call to another phone. To transfer the call, perform the following steps: 1. Hook-flash to get a dial tone. 2. Dial *90<phone-number> (e.g. *907401). After hearing the confirmation tone, you can hang up. The transferred call will hear a ringback tone, and the third-party phone (the one that the call has been forwarded to)_will be rung. When the third-party phone is picked up, the transferred call will be connected. If the third-party phone does not answer, the caller being transferred must hang up to cancel the connect attempt.

QoS - Quality of Service

The QoS function helps you to control your network traffic for each LAN (Ethernet and/or Wireless) application that accesses the WAN (Internet). It allows you to control the quality and speed of throughput for each application, when the system is running with a fully loaded upstream channel.

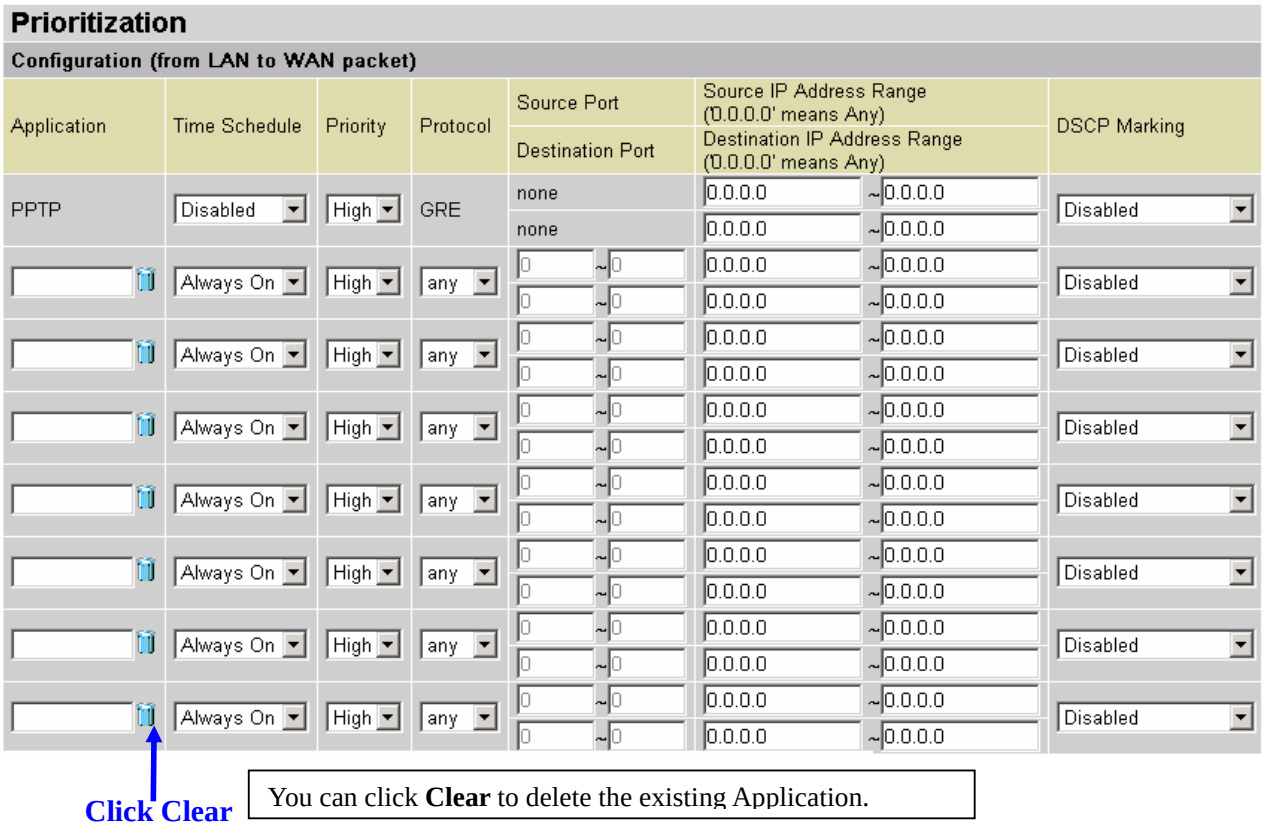
Here are the items within the **QoS** section: **Prioritization** and **Outbound / Inbound IP Throttling** (bandwidth management).

Prioritization

There are three priority settings provided in the Router:

- **High**
- **Normal** (Normal priority is the default for all traffic without any setting)
- **Low**

The ratio of utilization for each priority are: High (60%), Normal (30%) and Low (10%).



Application: A user-defined description identifying this new policy/application.

Time Schedule: The details of when this rule of your prioritization policy is active .

Priority: The priority given to this policy/application. The default setting is High; you may adjust this setting to fit your requirements.

Protocol: The name of the supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the backbone routers, based on the DSCP value. See Table 4. The DSCP Mapping Table:

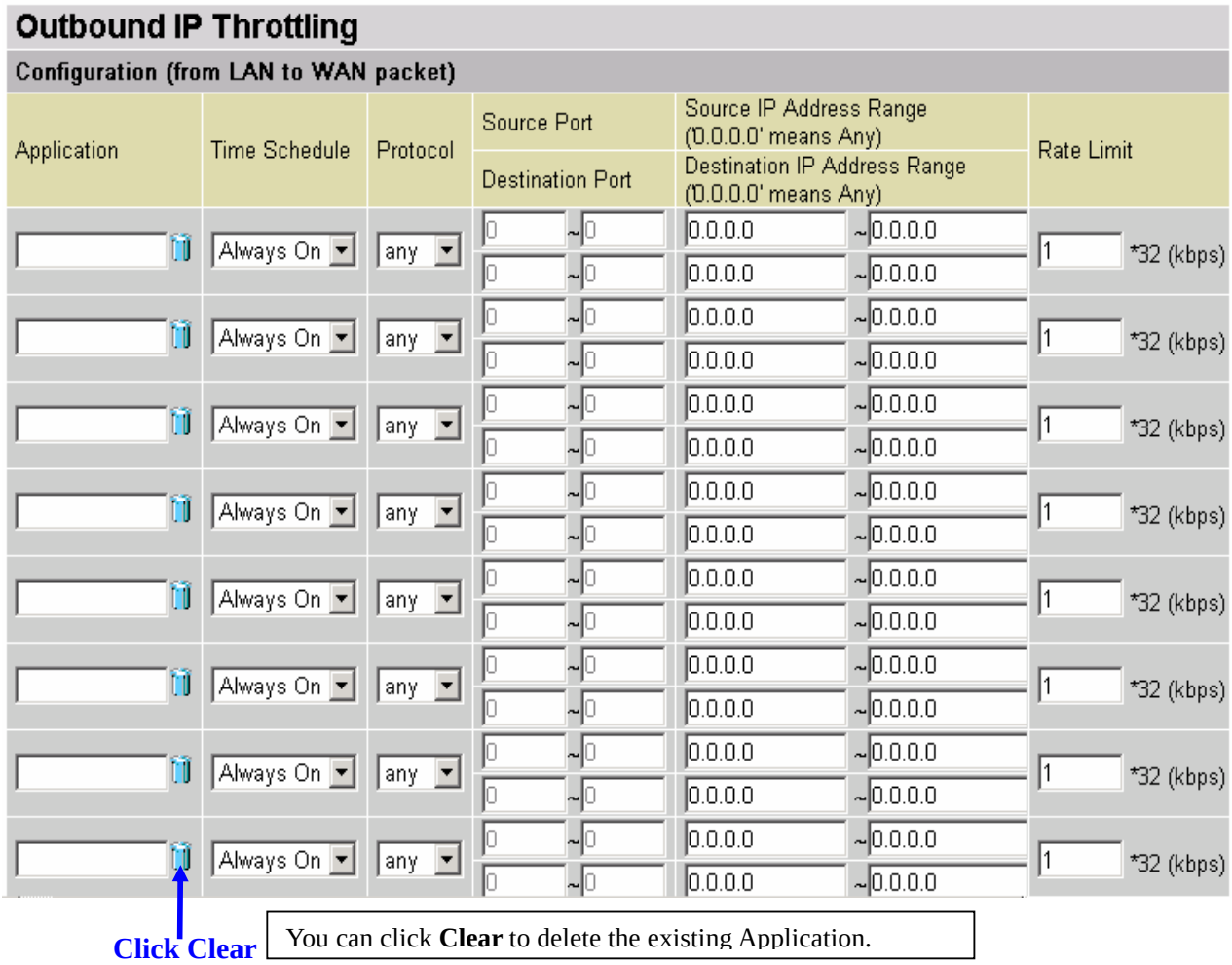
Note: To be sure all the routers on the backbones network have the capability of executing and checking DSCP so as to provide a QoS network.

Table 4: DSCP Mapping Table

DSCP Mapping Table	
ADSL Router	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Outbound IP Throttling (LAN to WAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the specified application to the specified value (Set in multiples of 32kbps.)



Application: A user-defined description to identify this policy/application.

Time Schedule: The details of when this rule of your prioritization policy is active. Refer to **Time Schedule** for more information.

Protocol: The name of the supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

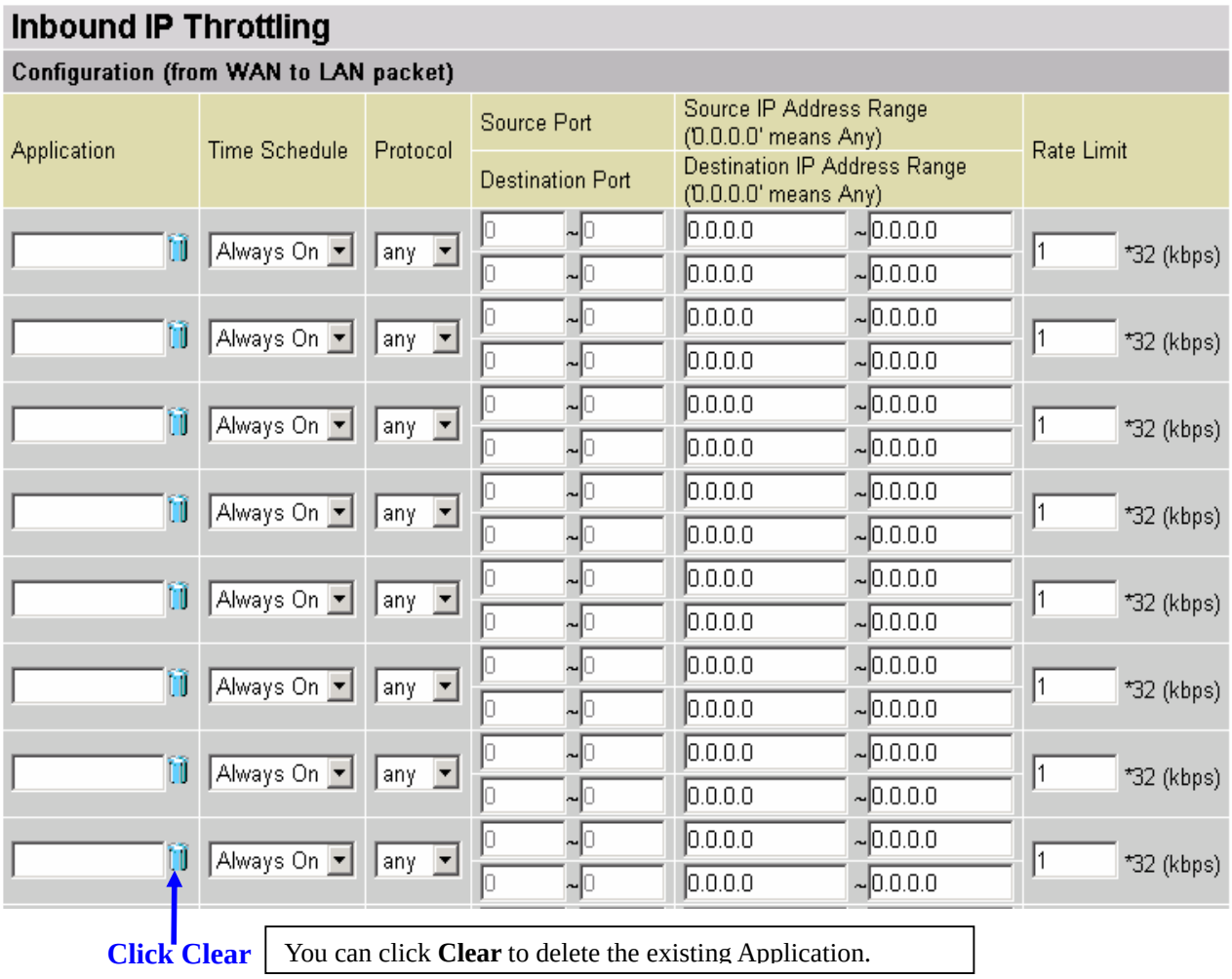
Source IP Address Range: The source IP address (or address range) of packets to be monitored.

Destination IP address Range: The destination IP address (or address range) of packets to be monitored.

Outbound Rate Limit: Used to limit the speed of outbound traffic (Set in multiples of 32kbps.)

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the specified application to the specified value (Set in multiples of 32kbps.)



Application: A user-defined description to identify this policy/application.

Time Schedule: The details of when this rule of your prioritization policy is active. Refer to **Time Schedule** for more information.

Protocol: The name of the supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

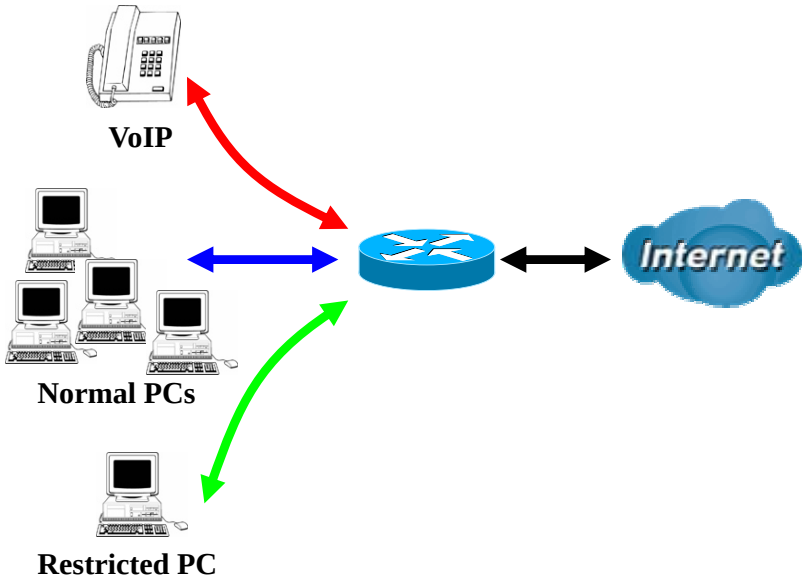
Source IP Address Range: The source IP address (or address range) of packets to be monitored.

Destination IP address Range: The destination IP address (or address range) of packets to be monitored.

Inbound Rate Limit: Used to limit the speed of inbound traffic (Set in multiples of 32kbps.)

Example: QoS for your Network

Connection Diagram



Information and Settings

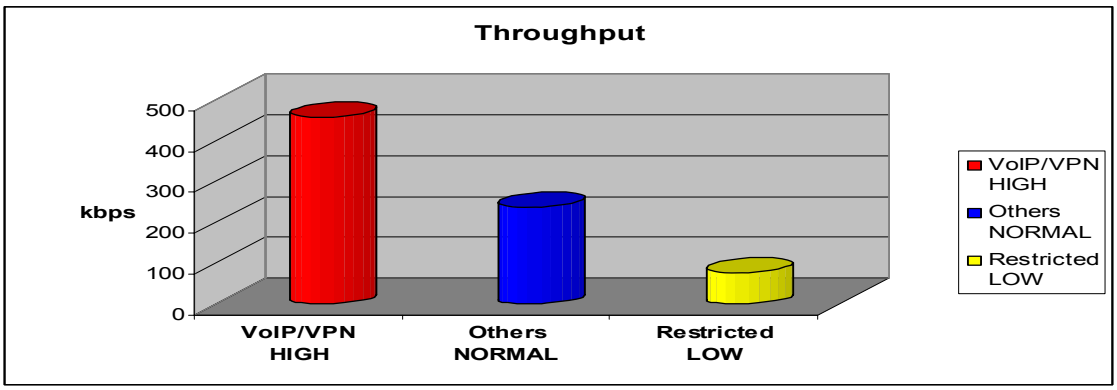
Upstream: 928 kbps
Downstream: 8 Mbps

VoIP User : 192.168.1.1
Normal Users : 192.168.1.2~192.168.1.5
Restricted User: 192.168.1.100

Prioritization

Configuration (from LAN to WAN packet)

Application	Time Schedule	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)	DSCP Marking
PPTP	Always On	High	GRE	none / none	0.0.0.0 ~ 0.0.0.0 / 0.0.0.0 ~ 0.0.0.0	Gold service (L)
VoIP	Always On	High	any	0 ~ 0 / 0 ~ 0	192.168.1.1 ~ 192.168.1.1 / 0.0.0.0 ~ 0.0.0.0	Gold service (L)
Restricted	TimeSlot1	Low	any	0 ~ 0 / 0 ~ 0	192.168.1.100 ~ 192.168.1.100 / 0.0.0.0 ~ 0.0.0.0	Gold service (L)



Mission-critical applications

Often, a VPN connection is a mission-critical application for exchanging data between Head and Branch offices.

This mission-critical application must be connected smoothly. without any dropping. To ensure this, you should set the priority to the high level to preventing any other applications from saturating the bandwidth.

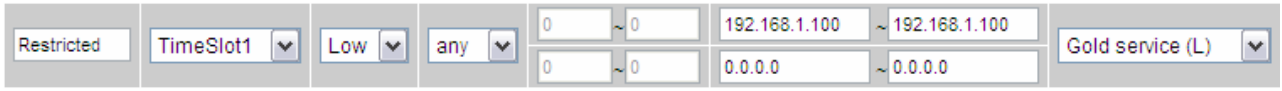
Voice applications

Voice applications are latency-sensitive. Most VoIP devices use the SIP protocol, which automatically assigns a port number. . This means that it is better to use a fixed IP address to catch VoIP packets and rout them as high priority traffic.

The settings shown above will help to improve the quality of your VoIP service when the link is fully loaded.

Restricted Application

Some users will setup a FTP server for downloading of their files by means of FTP.



The above settings will help to limit utilization of upstream bandwidth by the FTP connections. A time schedule can be implemented to limit file downloads to non-busy times.

Advanced setting by using IP throttling

With IP throttling you can specify more detail for bandwidth allocation; even if applications are located on the same level.

Upstream: 928kbps (29*32kbps)
Mission-critical Application: 192kbps (6*32kbps)
Voice Application: 128kbps (4*32kbps)
Restricted Application: 160kbps (5*32kbps)
Other Applications: 448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Application	Time Schedule	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)	Rate Limit
PPTP	Always On	gre	0 ~ 0	0.0.0.0 ~ 0.0.0.0	6 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
VoIP	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	4 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Restricted	TimeSlot1	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	5 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Others	TimeSlot1	any	0 ~ 0	192.168.1.2 ~ 192.168.1.5	14 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	

Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below will help you to limit bandwidth for such a application that needs restriction.

Inbound IP Throttling

Configuration (from WAN to LAN packet)

Application	Time Schedule	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)	Rate Limit
Restricted	TimeSlot1	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	64 *32 (kbps)
			0 ~ 0	192.168.1.100 ~ 192.168.1.100	

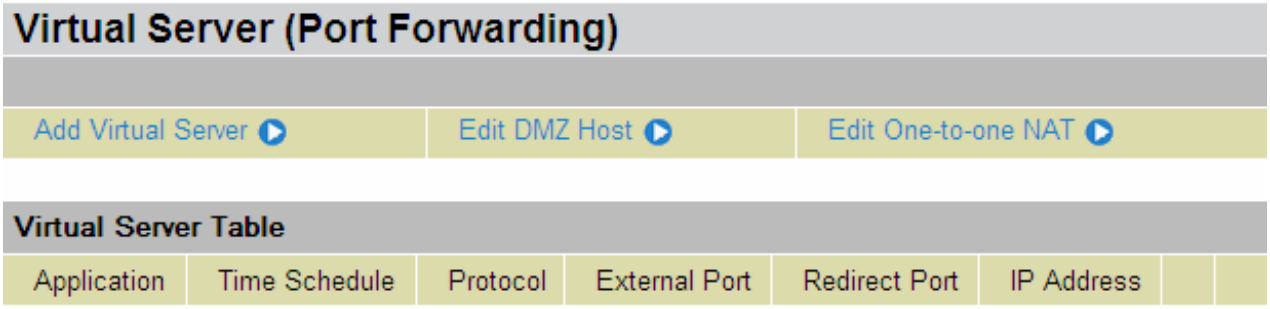
Virtual Server (known as Port Forwarding)

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which application program incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server, or any application (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) on your network that can be accessed from the WAN (i.e. from machines on the Internet that are outside your local network, and you are using NAT (Network Address Translation), then you will need to configure your router to forward these incoming connection attempts using specific ports to the computer on your network that is running the application/server. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

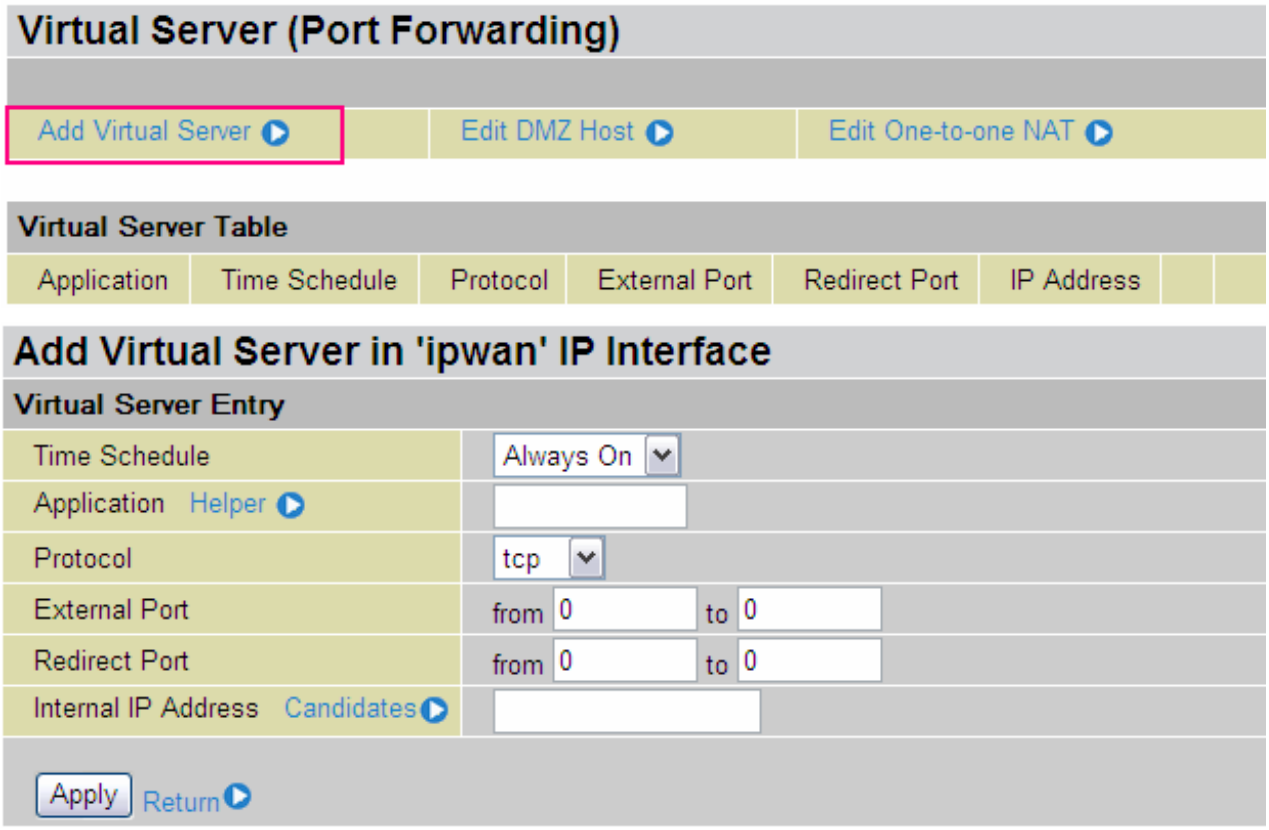
The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services on the routers public (WAN) IP address can be automatically redirected to local servers on the LAN network. Depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server within the LAN network



Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when NAT is enabled - all incoming connection attempts will point to your router unless you specifically created Virtual Server entries to forward those ports to a computer on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110), When an incoming access request for a specified port is received by the router, it will be forwarded to the corresponding internal server.



Time Schedule: The user-defined time period to enable your virtual server. You may specify a time schedule or Always on for the use of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

Application: A user-defined description used to identify this entry. You can click Helper to select existing predefined rules.

Helper**:** 20 predefined rules are available. Click the Radio button to select the rule; Application, Protocol and External/Redirect Ports will be automatically filled in after the selection.

Protocol: This is the protocol supported by the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

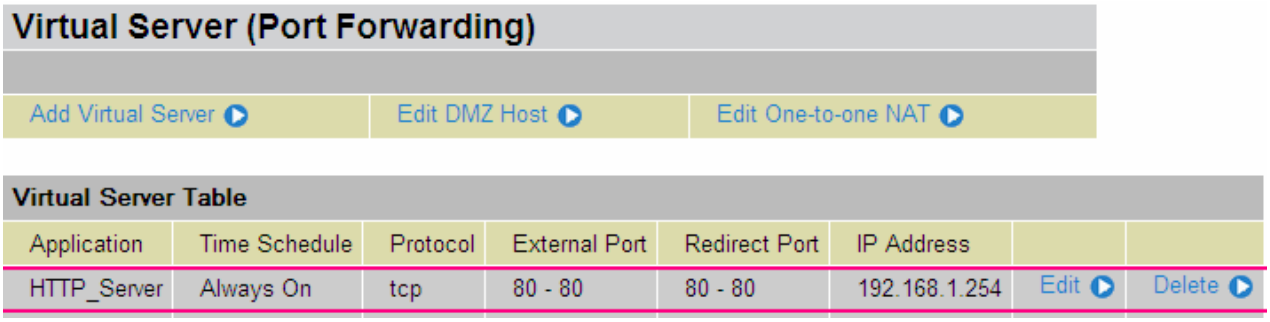
Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. Candidates List all existing computers currently connected to the network. You may assign a computer with an IP address or a MAC address from this list.

Example:

If you would like to remotely access your routers' Web/HTTP interface all the time, you would need to enable port number 80 (Web/HTTP) and map it to the Router's LAN IP Address. All incoming HTTP requests on the WAN network will then be forwarded to the router's IP address of 192.168.1.254. Since port number 80 is already a predefined rule, click **Helper** in the **Application** section**.** A predefined rules window will pop and you can select **HTTP_Sever**.

Application: *HTTP_Sever*
Time Schedule: *Always On*
Protocol: *tcp*
External Port: *80-80*
Redirect Port: *80-80*
IP Address: *192.168.1.254*



Edit: Click on this to edit this virtual server application.

Delete: Click on this to delete this virtual server application.

Using port forwarding has security implications, since outside users will be able to connect to Computers on your network. For this reason you are advised to add specific Virtual Server entries only for the ports that your application actually requires, instead of using the DMZ function. Using the DMZ function will result in all connection attempts from the WAN network having access to the public IP specified in the DMZ config section.

Attention

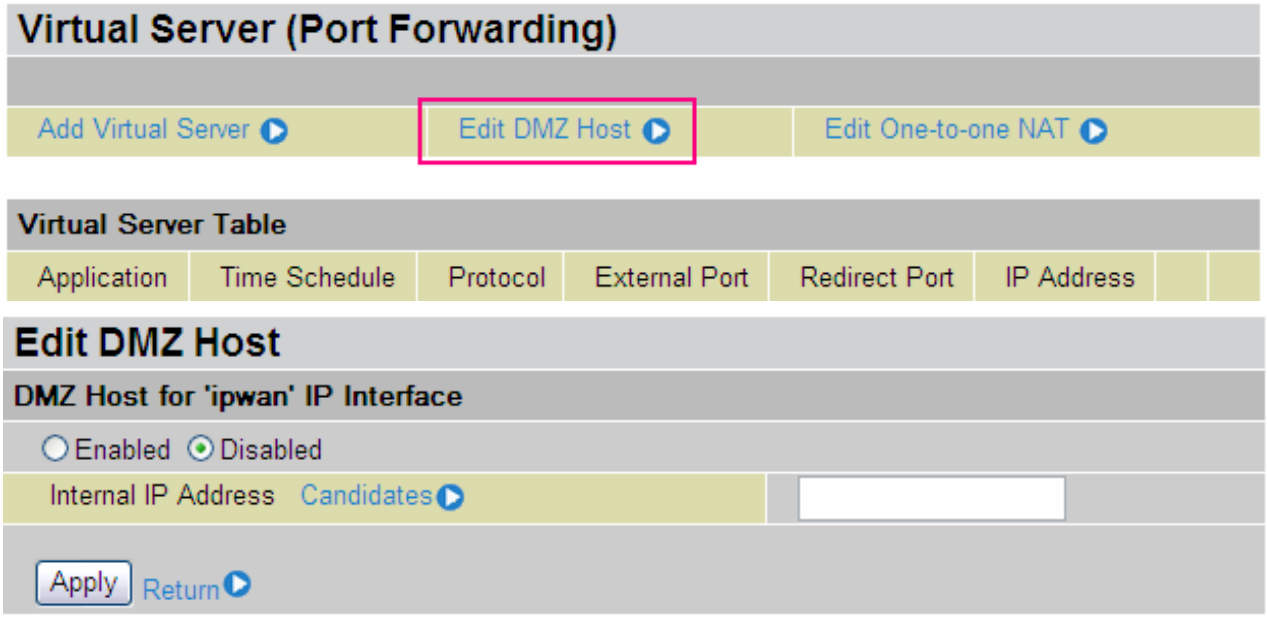
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will not work.

If the DHCP server option is enabled, you have to be very careful when assigning the IP addresses of virtual servers so that you avoid conflicting IP addresses. The easiest method of configuring Virtual Servers is to manually assign static IP address to each virtual server Computer, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. These manually configured IP addresses MUST still be in the same subnet as the router.

Edit DMZ Host

A DMZ Host is a computer on the LAN that is completely exposed to the Internet. When you have configured a particular internal IP address as the DMZ Host, all incoming packets will be checked by the routers firewall and NAT algorithms, and if the packet does not use a port number that has been assigned by any Virtual Server entry, it will be passed to the DMZ host

Cautious: This local computer, which is exposed to the Internet, may face a variety of security risks.you should make quite sure that it is adequately protected.



- **Disabled:** This option disables the DMZ function and is the default setting.
- **Enabled:** this option enables the DMZ function.

Internal IP Address: When the DMZ function is enabled, supply the static IP address of the DMZ Host. Be aware that this IP will be exposed to the WAN/Internet.

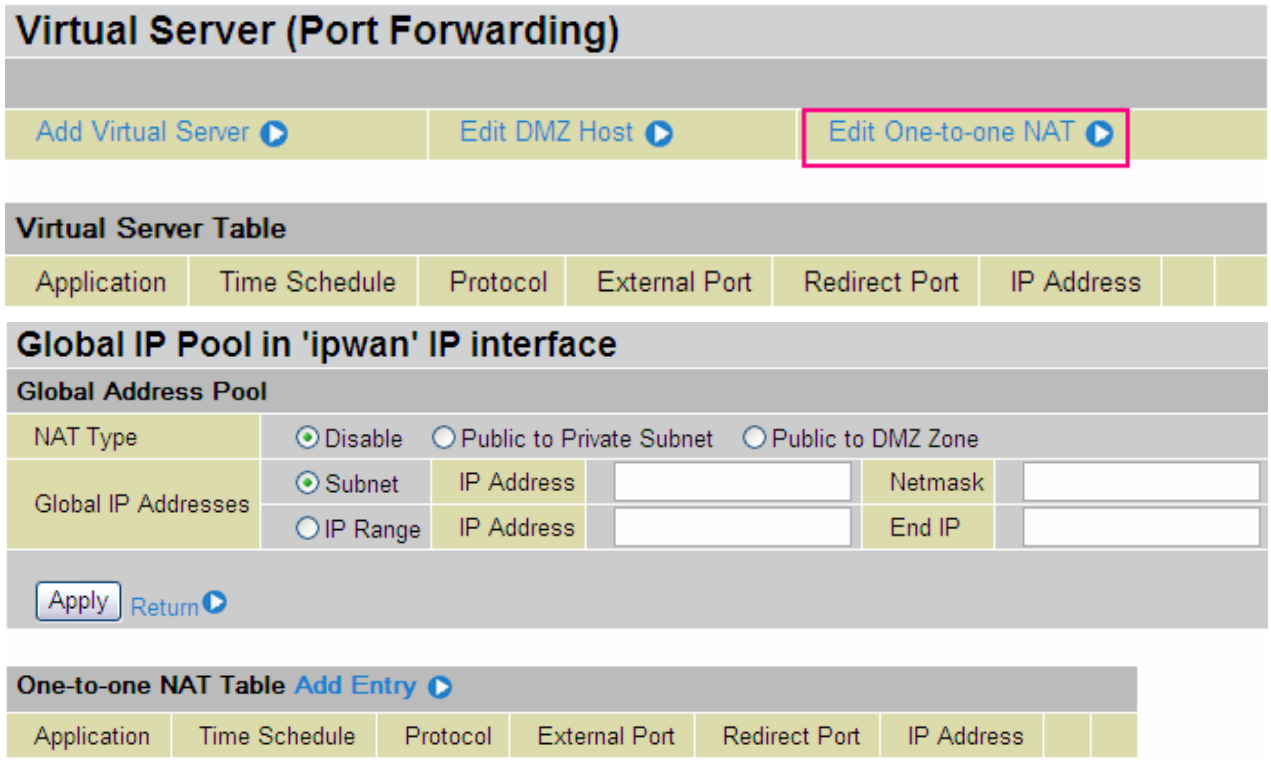
Candidates List all Computers currently connected to the network. You may assign a Compouter using its IP address and/or its MAC address from this list.

Select the **Apply** button to apply your changes.

Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private/local (LAN) IP address to a particular global/public (WAN) IP address.

If you have multiple public/WAN IP addresses provided by your ISP, you are will be able to use the One-to-One NAT function to utilize these IP addresses.



NAT Type: Select the desired NAT type. By default, the One-to-One NAT function is disabled.

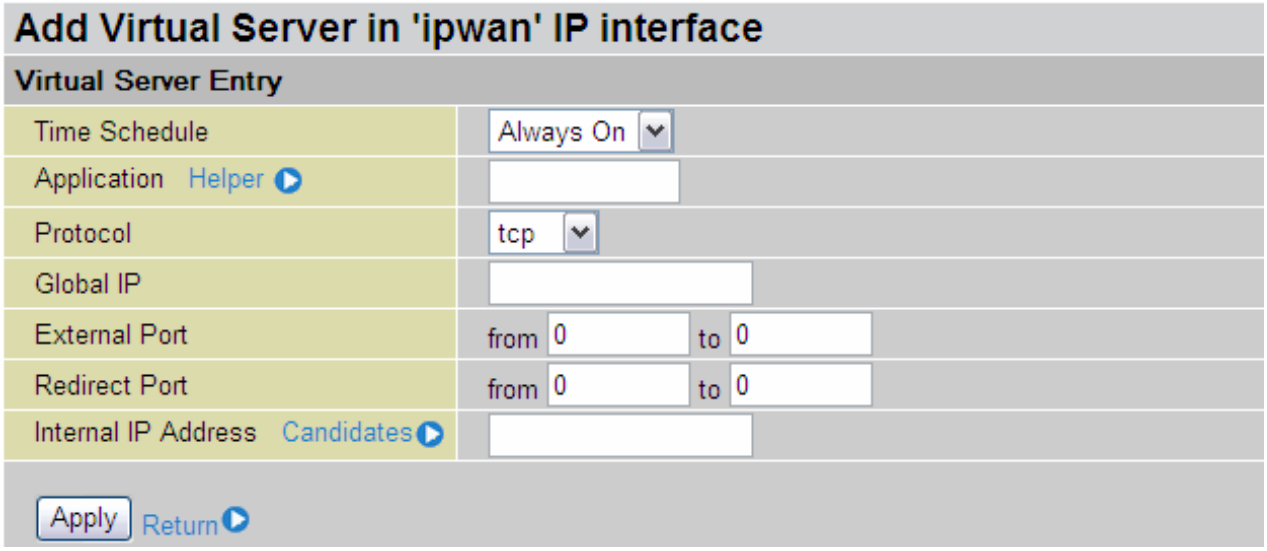
Global IP Address:

- **Subnet:** The subnet of the public/WAN IP addresses given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use the IP Range method to define your addresses.
- **IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Select the **Apply** button to apply your changes.

Click on

to create a new One-to-One NAT rule:



Time Schedule: The user-defined time period during which your virtual server is enabled. You may specify a time schedule or you can select **Always on** for this Virtual Server Entry. For setup and details, refer to the **Time Schedule** section

Application: This is a user-defined description to identify this entry. You can also click on Helper to select existing predefined rules.

Helper **:** 20 predefined rules are available. Click on the Radio button to select the rule; Application, Protocol and External/Redirect Ports will be filled after you make a selection.

Protocol: This is the protocol to be supported by the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP;

Global IP: Define a public/ WAN IP address for this Application to use.

External Port: The Port number on the Remote/WAN side that is used when accessing the virtual server.

Redirect Port: The Port number that the Local server on the LAN network will be listening on.

Internal IP Address: The private IP, on the LAN network, of the virtual server application. Candidates Lists all existing Computer connections on the network. You may assign a Computer by IP address or MAC address from this list.

Select the **Apply** button to apply your changes.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). Registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

For further information, please see IANA’s website at: http://www.iana.org/assignments/port-numbers

Table 5: Some Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Time Schedule

The Time Schedule function supports up to 16 time slots, helping you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely to real time. Since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. Your router time should correspond with your local time. If the time settings on you router are not set correctly, the Time Schedule will not function properly.

Time Schedule

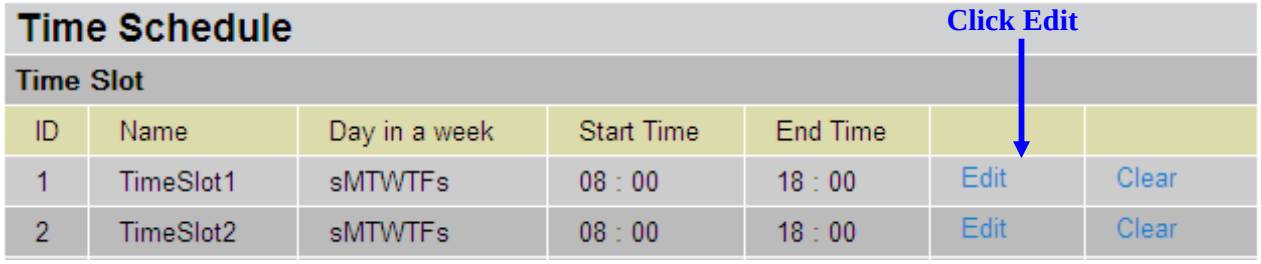
Time Slot

ID	Name	Day in a week	Start Time	End Time		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Edit	Clear
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Edit	Clear
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Edit	Clear
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Edit	Clear
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Edit	Clear
6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	Edit	Clear
7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	Edit	Clear
8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	Edit	Clear
9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	Edit	Clear
10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	Edit	Clear
11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	Edit	Clear
12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	Edit	Clear
13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	Edit	Clear
14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	Edit	Clear
15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	Edit	Clear
16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	Edit	Clear

Configuration of Time Schedule

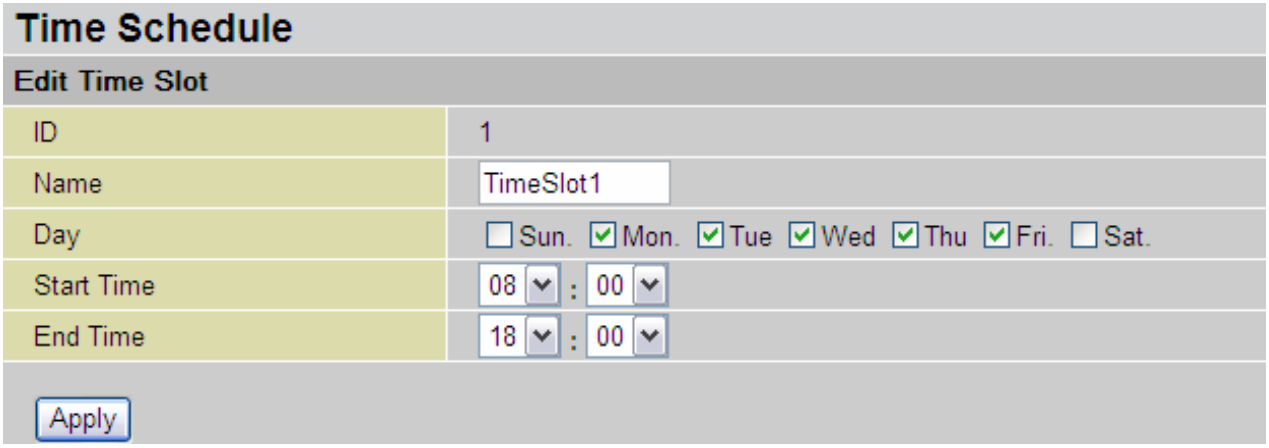
Edit a Time Slot

1. Choose any Time Slot (ID 1 to ID 16) to edit, click **Edit.**



Note: The days that you have selected will show as capital letters. Lower case letters show the day(s) that are not selected, and no rule will apply on these days.

2. The setting of this Time Slot will be shown in detail.



ID: This is the index of the time slot.

Name: A user-defined description identifying this time slot.

Day: The default setting is for Monday till Friday to be enabled. You should modify this according to your requirements.

Start Time: The default setting is 8:00 AM. You may specify any required start time for your schedule.

End Time: The default setting is 18:00 (6:00PM). You may specify any required end time for your schedule.

Select the **Apply** button to apply your changes.

Delete a Time Slot

Click **Clear** to delete the existing Time profile, i.e. Erase the selected Days and return to the default settings of Start Time / End Time.

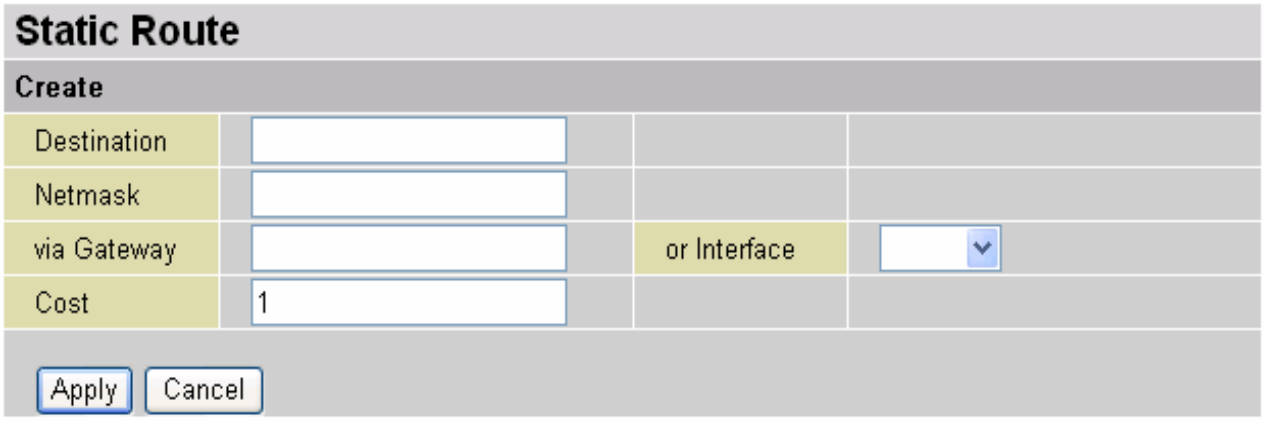
Advanced

The Configuration options of the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the **Advanced** section: **Static Route, Dynamic DNS**, **Check Email, Device Management, IGMP** and **VLAN Bridge.**

Static Route

Click on **Routing Table** and choose **Create Route** to add a routing table.



Destination: This is the destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses given above.

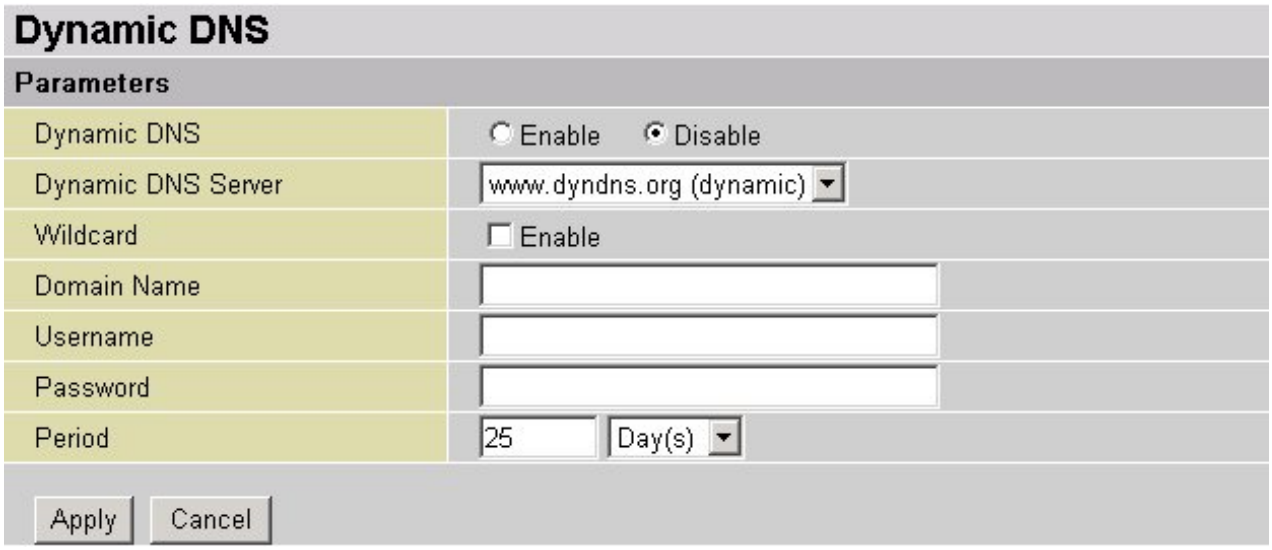
Gateway: This is the gateway IP address to which packets sent to the network defined above are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1 unless you know the actual path length.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/

There are more than 5 DDNS services supported.

- **Disable: S**elect this option to disable the Dynamic DNS function.
- **Enable: S**elect this option to enable the Dynamic DNS function. The following fields will be activated and must be filled in:

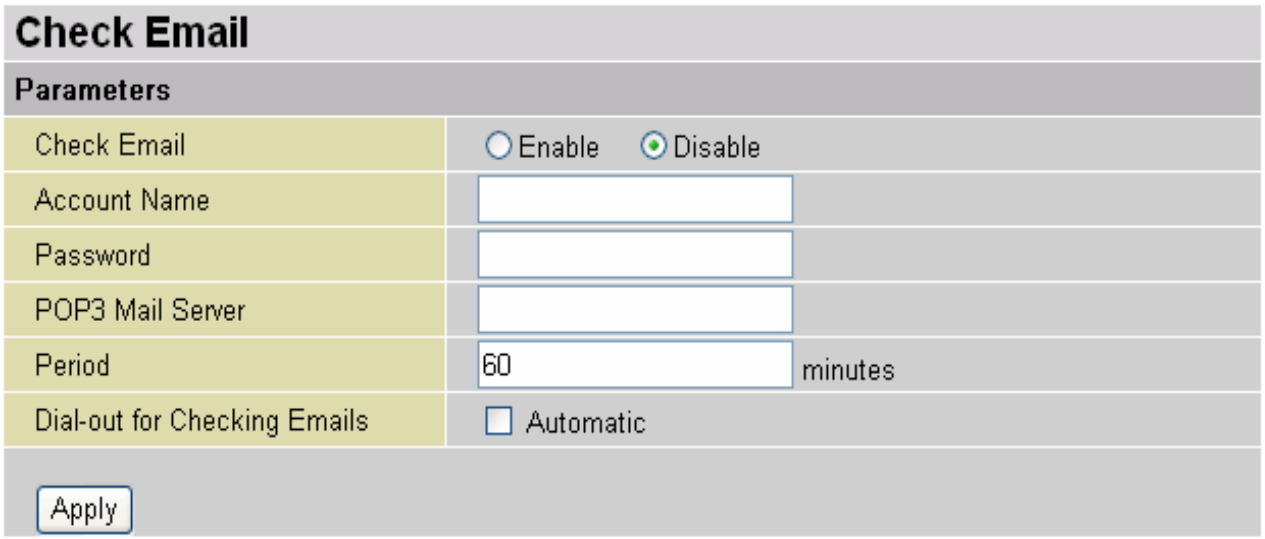
Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain Name, Username and Password: Enter your registered domain name and your username and password provided by your DDNS service.

Period: Set the time period between updates. This is the interval after which your router will exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Check Email

This function allows you to have the router check your POP3 mailbox for new Email messages You may view the status of this function using the Status – Email Checking section of the web interface, which also provides details on the number of new messages waiting. See the Status section of this manual for more information.



Check Email:

- **Disable: S**elect this option to disable the router's Email checking function.
- **Enable: S**elect this option to enable the routers Email checking function. The following fields will be activated and must be filled in:

Account Name: Enter the name (login) of the POP3 account you wish to check. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account's password.

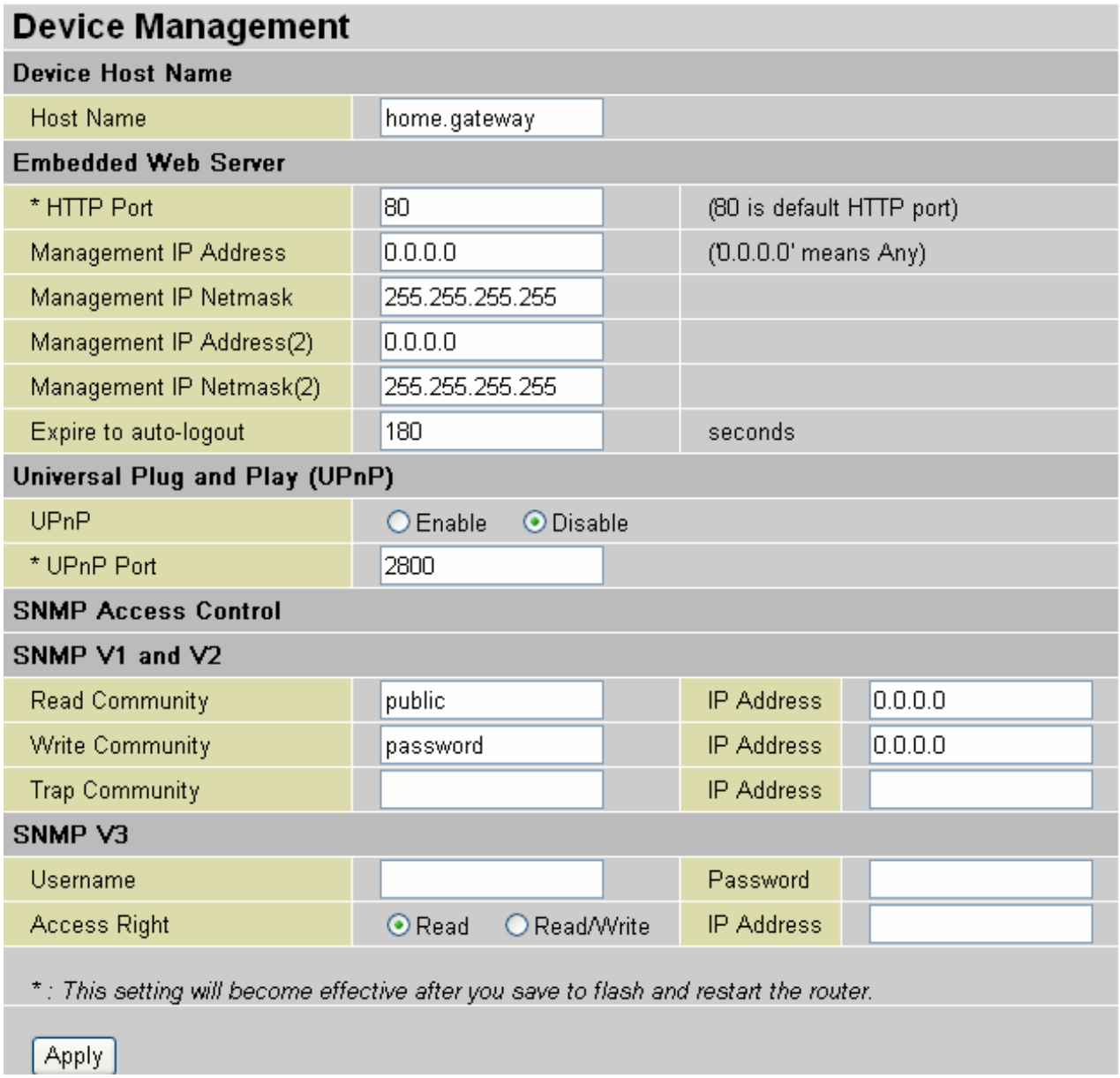
POP3 Mail Server: Enter your (POP) mail server name. Your Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Period: Enter the value in minutes between periodic mail checks.

Automatically dial-out for checking emails: When this function is enabled and your Internet connection is dropped, your ADSL router will automatically connect to your ISP to check for emails. Please be careful when using this feature if your ADSL service is charged by time online.

Device Management

The **Device Management** configuration settings allow you to control your router's security options and device monitoring features.



Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number of the router's embedded web server. (for web-based configuration) The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify the IP addresses allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

For Example: User A changes the routers HTTP port number to **100**, specifies their own IP address of**10.0.0.55**, and sets the logout time to be **100** seconds. The router will only allow User A access from the IP address **10.0.0.55** to logon to the Web GUI by typing: http://**10.0.0.2:100** in their web browser. After

100 seconds, the device will automatically logout User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal. On supported systems, it makes tasks such as port forwarding much easier by letting the application control the required settings, thus removing the need for the user to control the advanced configuration of their router.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

- **Disable: S**elect this option to disable the router's UPnP functionality.
- **Enable: S**elect this option to enable the router's UPnP functionality.

UPnP Port: The default port setting is 2800. It is highly recommended that users use this port value. If this value conflicts with other ports that are already being used, you may wish to change it.

SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, the user on this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users on this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users on this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access rights from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is a combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, providing authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

- ☑ System group
- ☑ Interfaces group

- ☑ Address Translation group
- ☑ IP group
- ☑ ICMP group
- ☑ TCP group
- ☑ UDP group
- ☒ EGP (not applicable)
- ☑ Transmission
- ☑ SNMP group

From RFC1650 (EtherLike-MIB):

- ☑ dot3Stats

From RFC 1493 (Bridge MIB):

- ☑ dot1dBase group
- ☑ dot1dTp group
- ☑ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

- ☑ pppLink group
- ☒ pppLqr group (not applicable)

From RFC 1472 (PPP/Security MIB):

- ☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- ☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- ☑ PPP Bridge Group

From RFC1573 (IfMIB):

- ☑ ifMIBObjects Group

From RFC1695 (atmMIB):

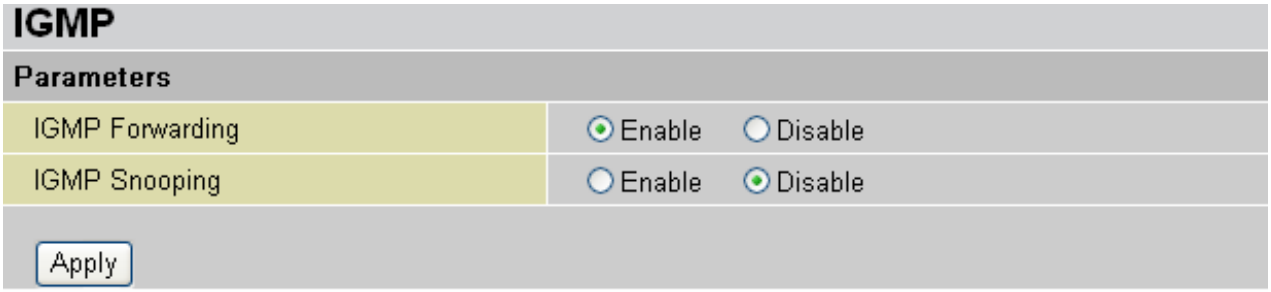
- ☑ atmMIBObjects

From RFC 1907 (SNMPv2):

- ☑ only snmpSetSerialNo OID

IGMP

IGMP, known as *Internet Group Management Protocol*, is used to management hosts from multicast group.

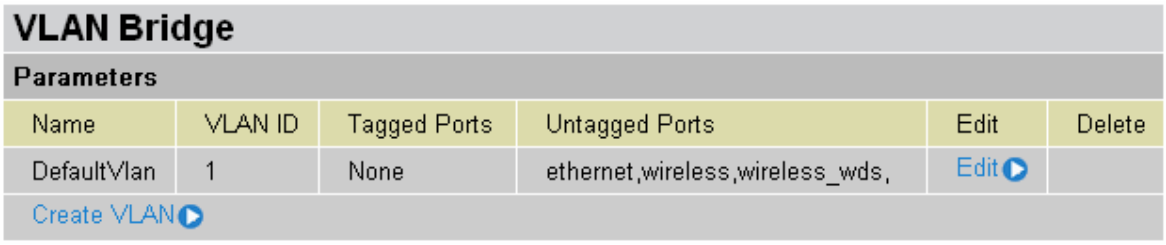


IGMP Forwarding: Accepting multicast packet. Default is **Enable.**

IGMP Snooping: Allowing switched Ethernet to check and make correct forwarding decisions. Default is **Disable.**

VLAN Bridge

This section allows you to create VLAN group and specify the members.



Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Advanced VLAN Setup Example (Triple Play)

VLAN_data:
Ethernet Port 1, Wireless and Wireless WDS are reserving for Internet
- On Ethernet port 1, VC 0/40 bridged mode is also required.

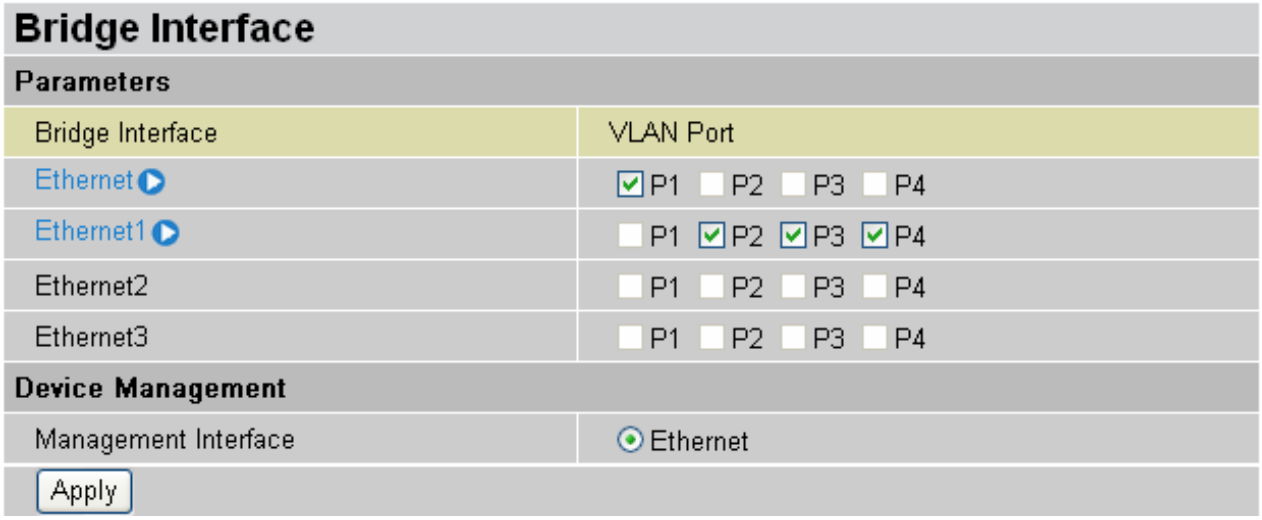
VLAN_Video
Ethernet ports: 2, 3 and 4:
- 0/33 Bi-directional IP
- 0/34 Video
- 0/35 Video
- 0/36 Video Subscriber Services (EPG, EAS, etc.)
- 0/37 Video
- 0/38 Video
- 0/39 Spare

Step 1: Setup Member Ports

Go to **Configuration → LAN → Bridge Interface.**
You can setup member ports for each VLAN group under Bridge Interface section. From the example, two

VLAN groups need to be created.
Ethernet: P1 (Port 1)
Ethernet1: P2, P3 and P4 (Port 2, 3, 4) Please deselect P2, P3, P4 from Ethernet VLAN Port first.
Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4



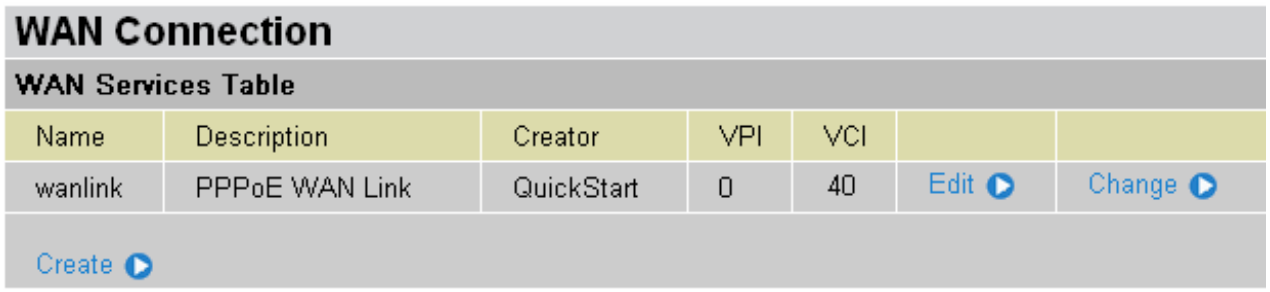
Step 2: Create WAN Interface

Go to **Configuration → WAN→ ISP**

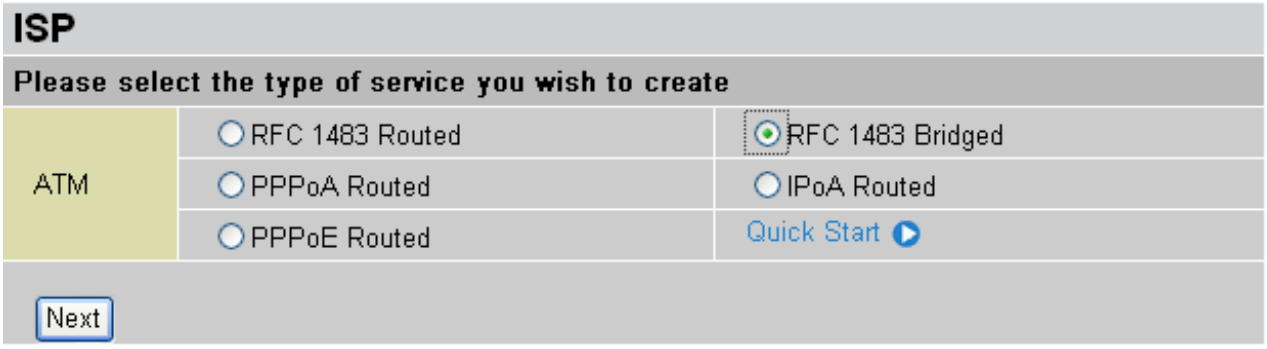
wanlink is the factory default WAN interface which is used for data/internet access. If your ISP uses this access protocol, click **Edit** to input other parameters if needed. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

From the example, 0/40 is used for data/internet and assumes PPPoE is used; click the **Edit** to change the VPI/VCI to 0/40. In South Africa, we use 8/35 for data by default.

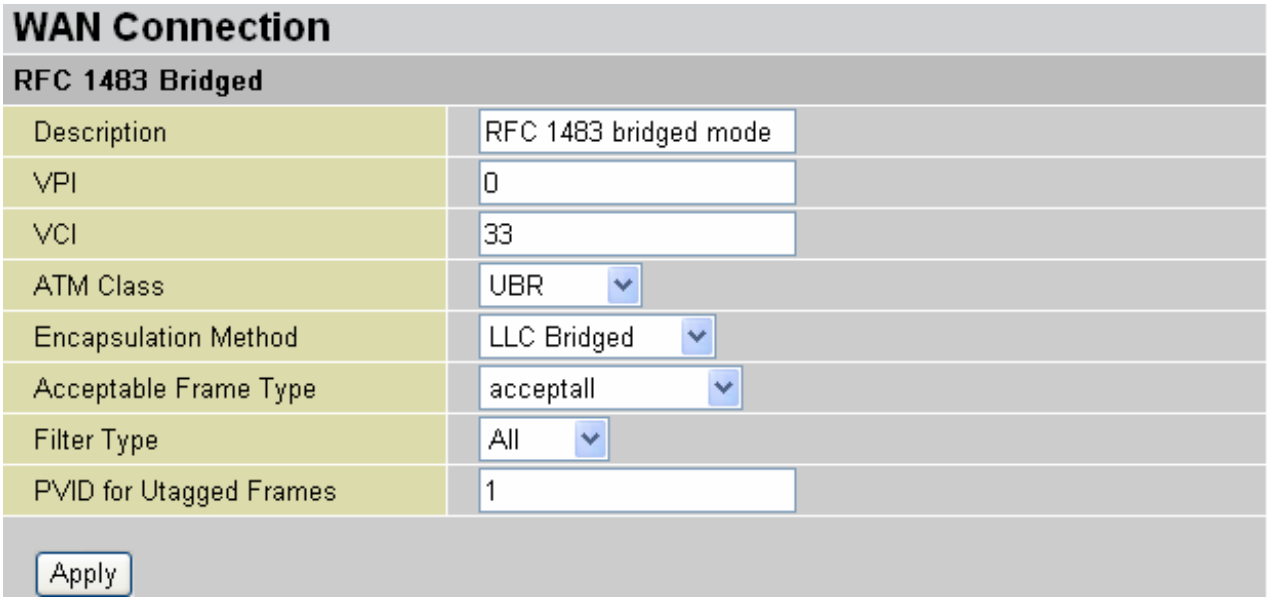
Click **Create** to setup up additional WAN interface for video applications. Total of 8 VLAN's are supported; therefore, only 8 WAN interfaces can be created in the table.



From the example, PVC 0/33 to 0/39 are assigned for video using 1483 Bridged mode. select **RFC 1483 Bridged** and click **Next** to continue the setup.



Spaces next to VPI and VCI, type 0 and 33 in respectively. Select appropriate ATM Class, Encapsulation Method, Acceptable Frame Type, Filter Type and PVID for Untagged Frames.



VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

Acceptable Frame Type: Specify what kind of traffic can use this connection, all traffic or only VLAN tagged.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

PVID for Untagged Frames: Port VLAN Identifier is known as PVID. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID.

From the example, only the VPI and VCI section need to be filled-in, just leave the rest as is. Repeat the same procedure by clicking **Create** → select **RFC1483 Bridged** → fill-in the rest of PVC 0/34 to 0/39.

WAN Connection

WAN Services Table

Name	Description	Creator	VPI	VCI		
wanlink	PPPoE WAN Link	QuickStart	0	40	Edit	Change
rfc1483-0	RFC 1483 bridged mode	WebAdmin	0	33	Edit	Delete
rfc1483-1	RFC 1483 bridged mode	WebAdmin	0	34	Edit	Delete
rfc1483-2	RFC 1483 bridged mode	WebAdmin	0	35	Edit	Delete
rfc1483-3	RFC 1483 bridged mode	WebAdmin	0	36	Edit	Delete
rfc1483-4	RFC 1483 bridged mode	WebAdmin	0	37	Edit	Delete
rfc1483-5	RFC 1483 bridged mode	WebAdmin	0	38	Edit	Delete
rfc1483-6	RFC 1483 bridged mode	WebAdmin	0	39	Edit	Delete

Step 3: Setup VLAN Service

Go to **Configuration → Advanced → VLAN Bridge**

DefaultVlan lists all member ports. It is necessary to group specific member ports for each VLAN.

From the example, two VLAN groups are requested: Data and Video.

To create another VLAN group for Video, click on **Create VLAN.**

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit	

Create VLAN

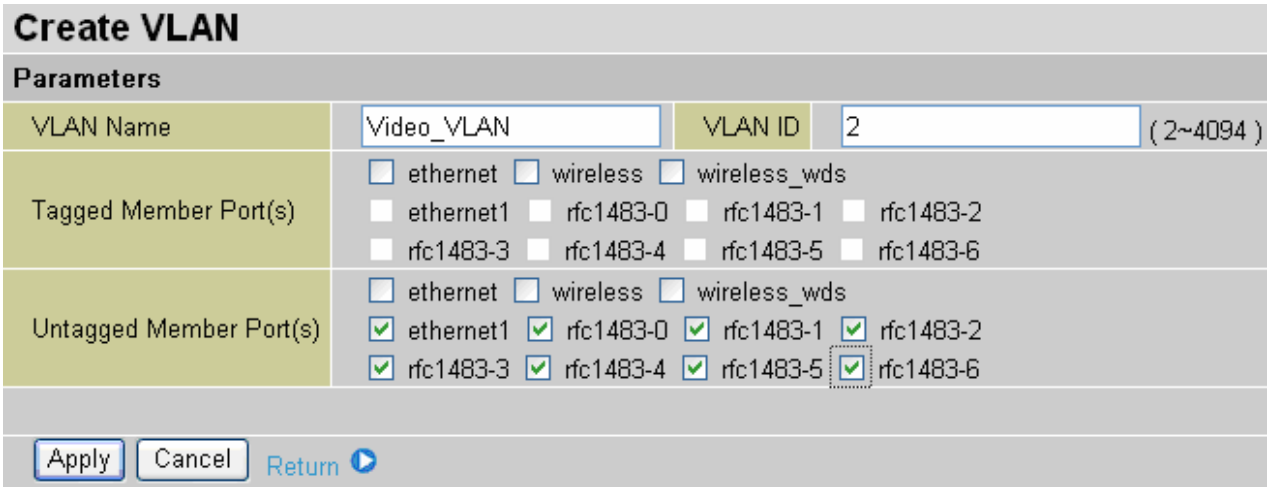
Give a name and ID (PVID) to identify the Video group. The valid value range for PVID is 1 ~ 4094.

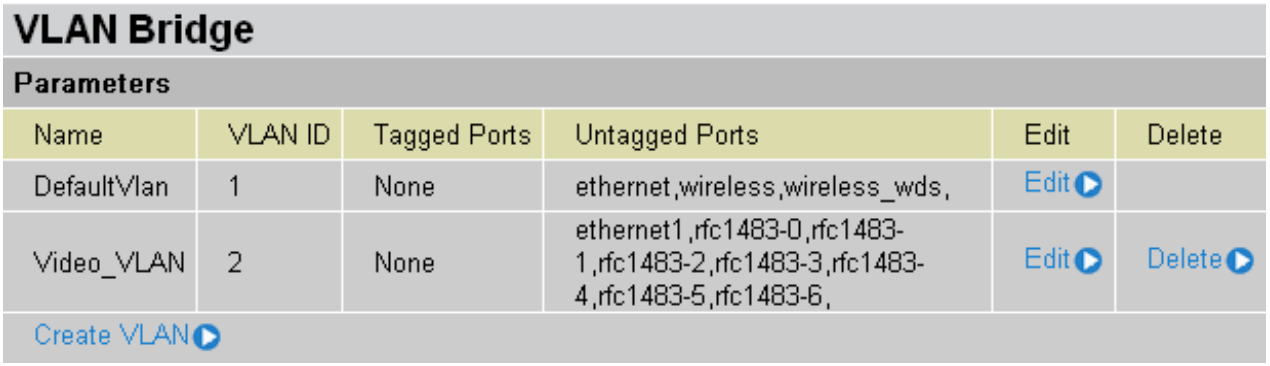
From the example:

VLAN untagged ports for Data/Internet: Ethernet, wireless and wireless_wds.

VLAN untagged ports for Video: ethernet1, rfc-1483-0 ~ rfc-1483-6.

Click **Apply** to made change effective immediately.



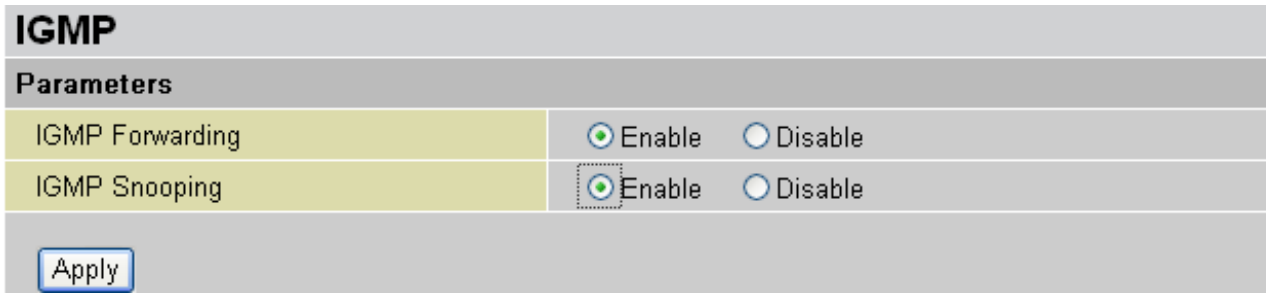


Having mapped the **VLAN Bridge** with the **Bridge Interface** created in Step1, you will see the comfortable relationship in these two screenshots.

Step 4: IGMP Snooping Enable

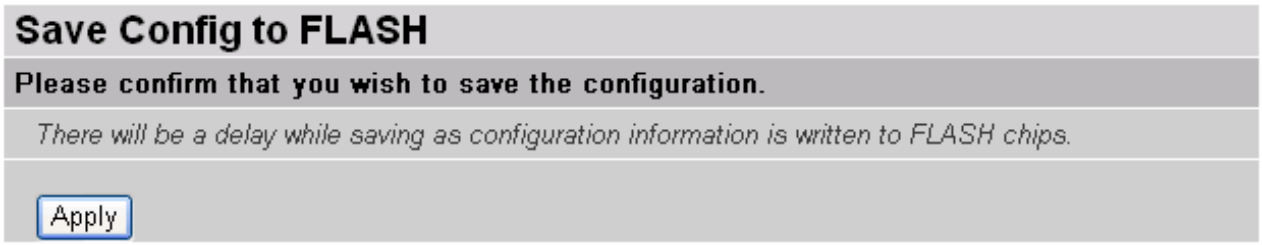
Select **Configuration → Advanced → IGMP**.

IGMP Snooping must be enabled in order to allow the video stream forwarding to correctly function.



Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid them from being lost after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.


Save Config to FLASH
Please confirm that you wish to save the configuration.
There will be a delay while saving as configuration information is written to FLASH chips.
Apply

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting the Help desk .

Problems starting up the router

Problem	*Corrective Action*
None of the LEDs are on when you turn on the router.	Check the connection between the power adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with the WAN Interface

Problem	*Corrective Action*
Initialization of the PVC connection ("linesync") failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router. If you still have problems, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket, and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Problems with the LAN Interface

Problem	*Corrective Action*
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
	Verify that the IP address and the subnet mask are consistent between the router and the workstations.

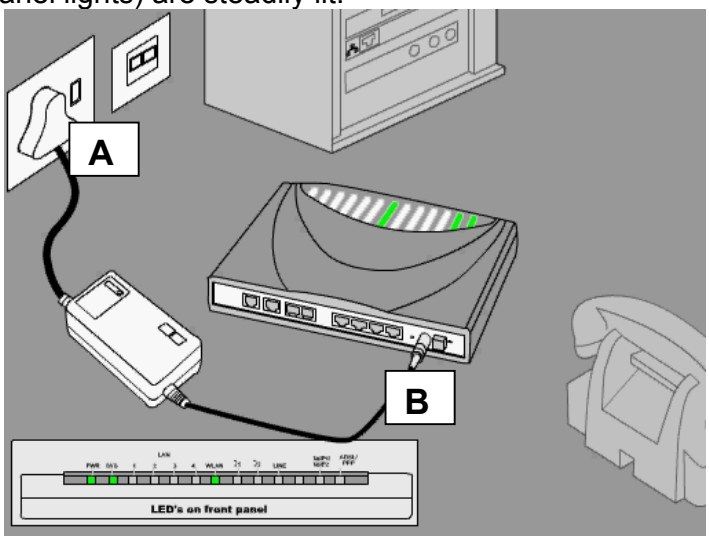
APPENDIX A: Windows 98 setup

Installation & Setup: (Windows 98, 98SE, ME or NT4)

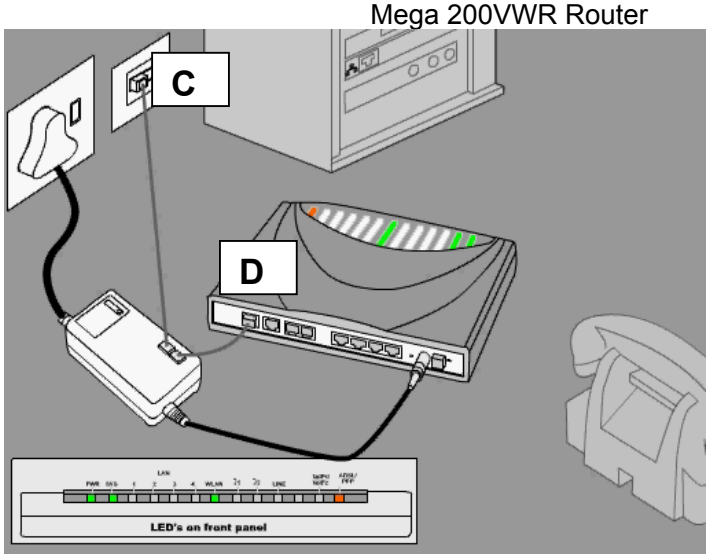
Hardware Installation:

Follow the installation instructions below, referring to the images provided for each step. Also note the hardware overview diagram (Figure 1) and the corresponding letter indicators.

1. **Power up the device**
   a) Plug the power adapter into the electrical wall-socket **(A).**
   b) Plug the power pin-connector (male) into the router's power socket **(B).**
   c) Switch the router on.
   d) Wait approximately 1 minute, then confirm that the "PWR" and "SYS" LED's (front panel lights) are steadily lit.



2. **Connect the ADSL line**
   a) Connect one of the included (grey) telephone cable between the Telkom wall-socket and one of the sockets on the integrated power and surge unit **(C)**.
   b) Connect the other included (grey) telephone cable between the remaining unused socket on the integrated power and surge unit and the router's "ADSL" port **(D)**.



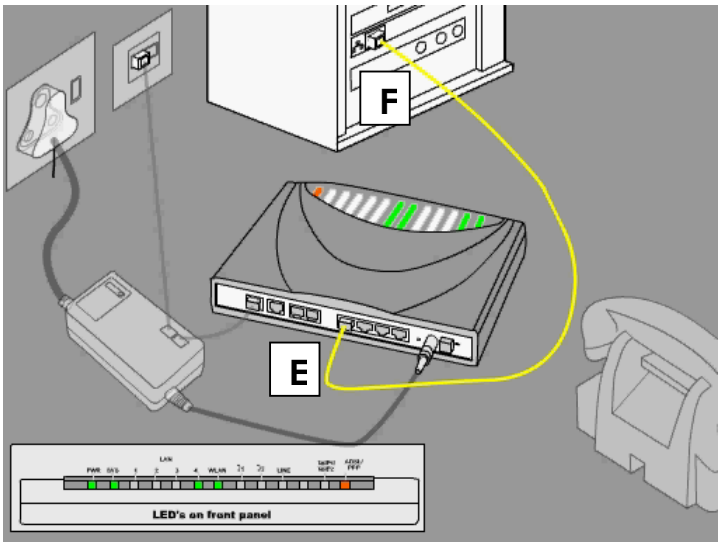
c) Your router will now attempt to synchronize with the Telkom ADSL line. The "ADSL/PPP" LED will start to blink green and after approximately 1-2 minutes be steadily lit orange. If the "ADSL/PPP" LED does not become lit, please refer to the troubleshooting section at the end of this guide.

d) The Mega 200VWR router is, by default, distributed with a guest ISP username and password. This guest account allows you access to the www.telkom.co.za website only. Although this account only allows limited access, it serves as a tool to confirm that your hardware installation and your own PC's network configuration has been completed successfully. This guest account will cause your router's "ADSL/PPP" LED to be steadily lit orange now. We will again refer to this guest account at a later stage of the installation process.

3. Connect the LAN (network) cable

a) Plug one end of the enclosed (yellow) Ethernet (CAT-5 LAN) cable into one of the router's LAN ports, you may choose any of the 4 ports **(E)**.

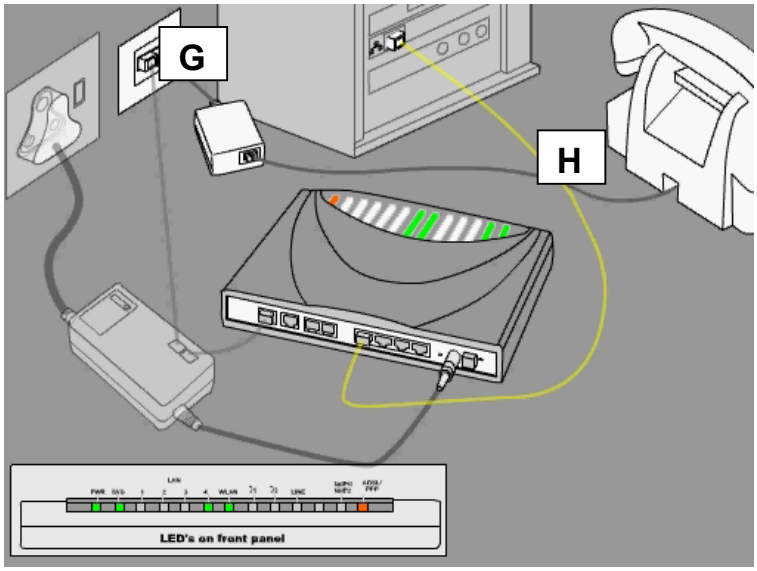
b) Plug the other end of the Ethernet (CAT-5 LAN) cable into your computer's network port or network hub/switch **(F)**.



c) Confirm that the corresponding LAN LED is lit. If it is not lit, you may have plugged the cable into the wrong port on the back panel of your PC.
d) You can connect up to 4 network devices directly to the Mega 200VWR.

4. Connect the ADSL micro filters

a) If you also intend to use traditional telephones (for normal voice calls) on the ADSL line, you need to connect the included ADSL micro filters. (These units filter out any data noise on your voice lines.) **Note that this setup is not for VoIP calls, but traditional analog voice calls on your ADSL line. These calls are charged separately.**
b) Plug the micro filter into the remaining Telkom ADSL wall-socket. **(G)**.
c) Plug the telephone into the micro filter using the included (grey) telephone cable. **(H)**



d) Important Note: Make sure that you do not connect any micro-filters between the Telkom wall socket used for the router and the router itself. Refer to the route indicated by **(C)** and **(D)** below.

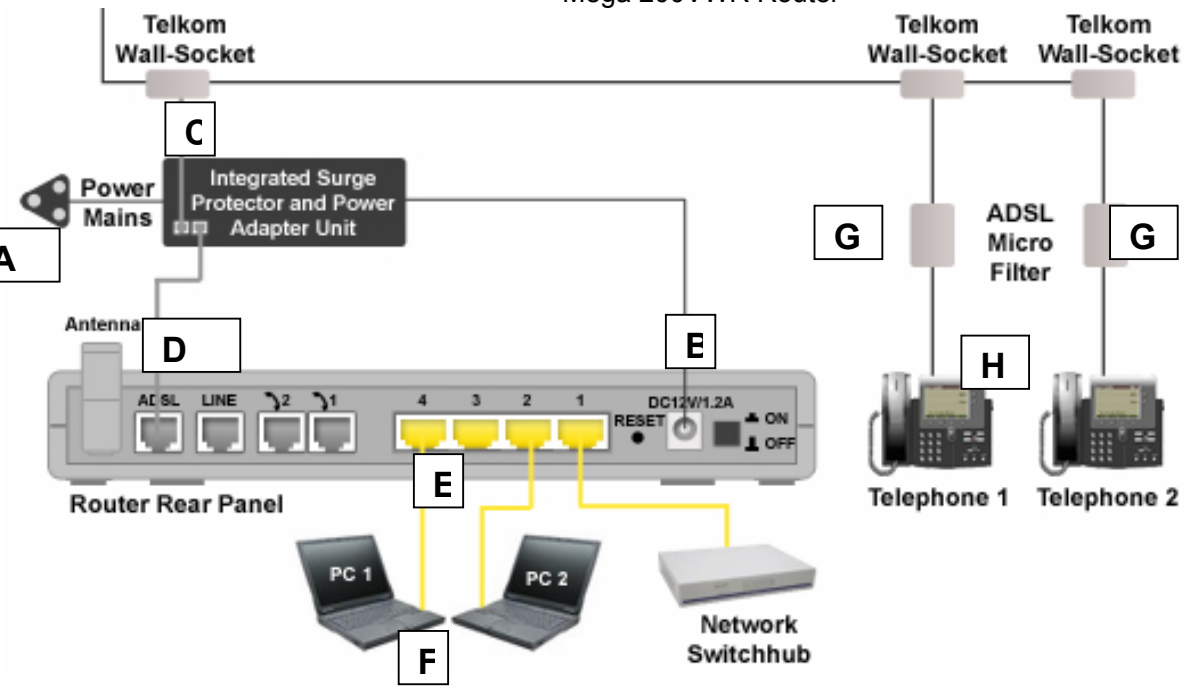


Figure 1

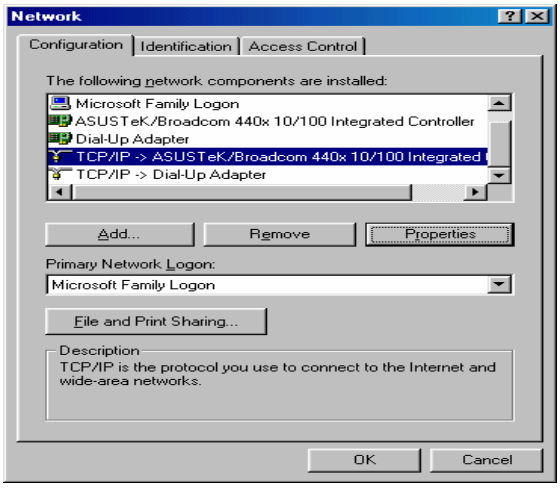
NOTE:

- ✓ Step 4 above is used when you still want to be able to use your ADSL line to make normal traditional analog calls.
- ✓ Setting up your Mega 200VWR hardware to be able to make VoIP calls will be covered later in the Quick Start Guide.
- ✓ Please refer to the the VoIP section of this online manual for further information pertaining to VoIP.

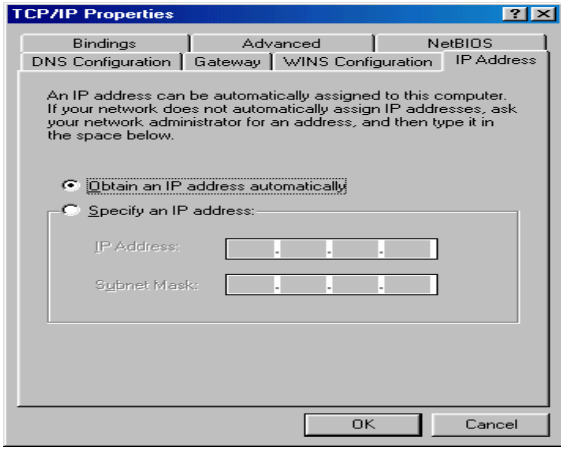
Network Card Configuration:

Using Windows 98/ME:

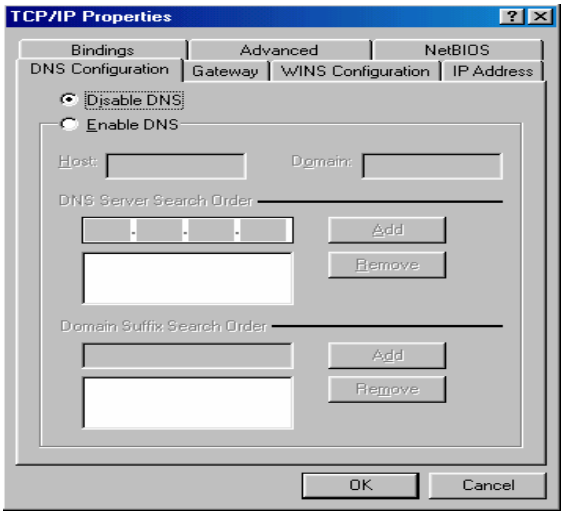
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP -> NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.



3. Select the **Obtain an IP address automatically** radio button.

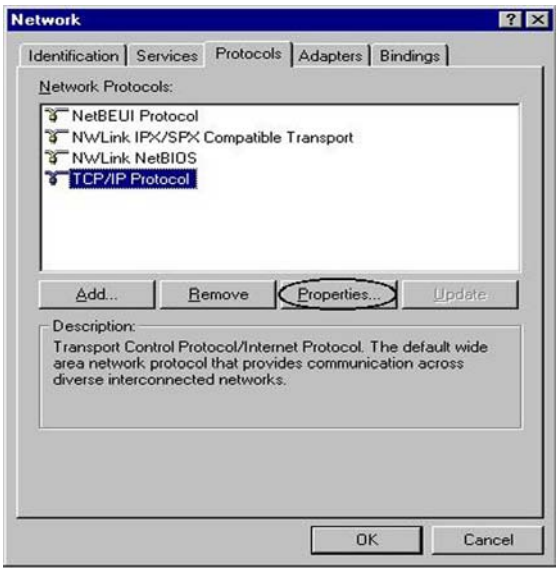

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK**.
6. Click **OK** again to finish the configuration.

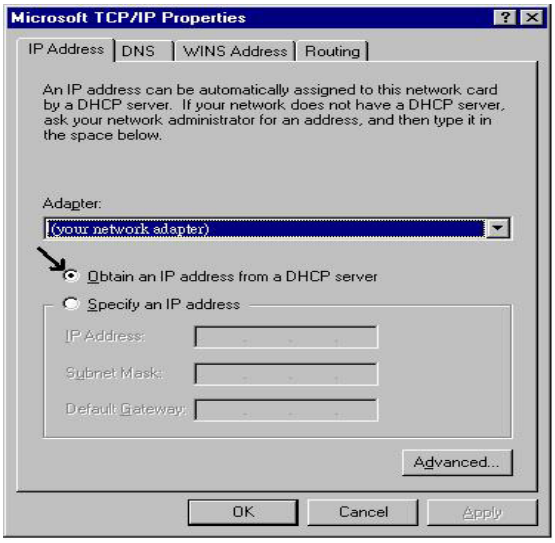


Using Windows NT4.0:

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button.
4. Now select the **DNS** tab and make sure that no DNS is specified.
5. Click **OK** to close **TCP/IP Properties.**
6. Click **OK** again to close the **Network** window**.**


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
(your network adapter)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

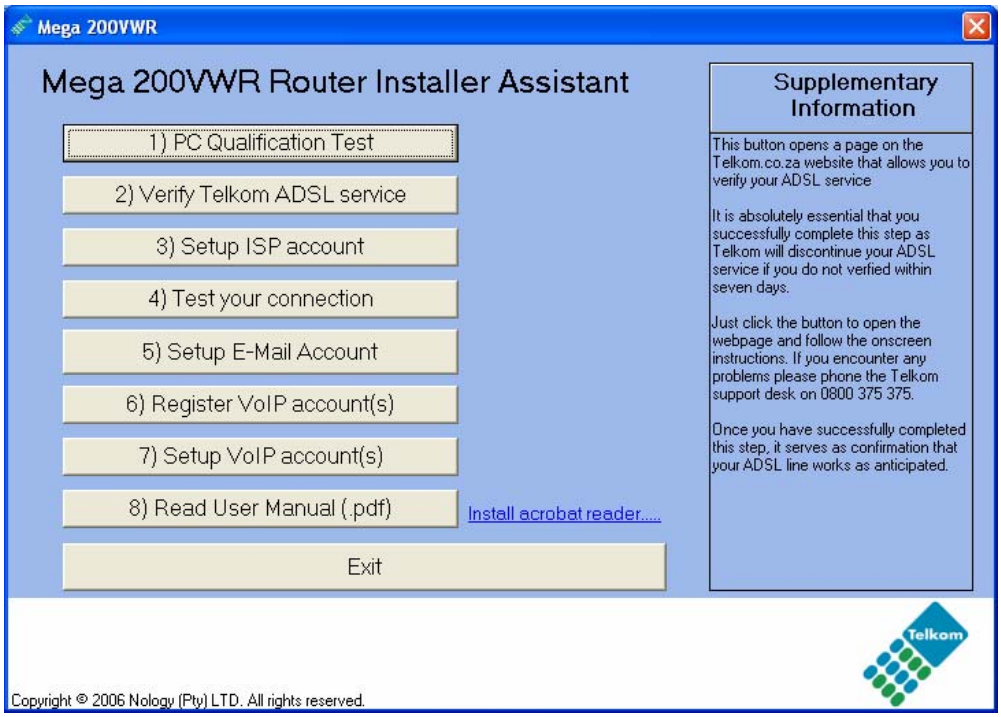
Router Setup and miscellaneous tasks:

In this section you will:

1) Verify that your computer meets the minimum requirements for Telkom ADSL
2) Verify your Telkom ADSL service on the Telkom website
3) Setup your own ISP account on your Mega 200VWR router
4) Test your Internet connection by opening a webpage
5) Setup E-Mail account in Outlook Express (optional)
6) Request VoIP account(s) on the Telkom VoIP website (optional)
7) Setup VoIP account(s) on your Mega 200VWR (optional)
8) Read this manual. (optional)

✓ It is crucially important to read the supplementary information supplied on the right side of the auto run menu. It supplies valuable information on how to use the menu and explains the function of each step and button.

If you have not already inserted the CD and launched the menu below, please do so now.
A menu screen will be displayed as shown in figure 2 below.


Mega 200VWR
Mega 200VWR Router Installer Assistant
1) PC Qualification Test
2) Verify Telkom ADSL service
3) Setup ISP account
4) Test your connection
5) Setup E-Mail Account
6) Register VoIP account(s)
7) Setup VoIP account(s)
8) Read User Manual (.pdf)
Install acrobat reader.....
Exit
Supplementary Information
This button opens a page on the Telkom.co.za website that allows you to verify your ADSL service
It is absolutely essential that you successfully complete this step as Telkom will discontinue your ADSL service if you do not verfied within seven days.
Just click the button to open the webpage and follow the onscreen instructions. If you encounter any problems please phone the Telkom support desk on 0800 375 375.
Once you have successfully completed this step, it serves as confirmation that your ADSL line works as anticipated.
Telkom
Copyright © 2006 Nology (Pty) LTD. All rights reserved.
Figure 2

✓ If nothing happens when you insert the CD, please refer to the troubleshooting section at the end of this section.

Please complete steps 1 through 8 as listed below:

1) **Verify that your computer meets the minimum requirements for Telkom ADSL:**
   Click the "PC Qualification Test" button on the menu screen. A diagnostic program will open to verify that your PC meets the minimum requirements. Just follow the instructions and when complete, close the program to return to the menu screen and proceed to the next step.

   If you encounter any problems or have any questions, please contact the helpdesk for which the contact information is provided in the last section of this quick start booklet.

2) **Verify your ADSL service on the Telkom website:**
   Click the 'Verify Telkom ADSL service' button. Your web-browser will now open and attempt to connect to the Telkom ADSL service verification page. Once the site is fully displayed, follow the on-screen instructions to complete your ADSL service verification. Once you have done this, close the web browser and return to the menu screen.

- ✓ **It is imperative that you verify your ADSL service on this webpage within seven days of line installation/conversion. If you do not, Telkom will cancel your ADSL service.**
- ✓ If you are using the Internet browser for the first time, it will prompt you to complete a few simple setup tasks.
- ✓ If you are unable to view the Telkom verification webpage, please make sure that you have performed the previous steps (hardware setup and network card setup) of this quick setup guide correctly. If the problem persists, contact technical support.

3) **Setup your own ISP account on your Mega 200VWR router:**

Important Information

- ✓ Before you continue, make sure that you do not have any active software firewalls running. These include programs like: Norton Internet Security, TrendMicro's PC-Cillin, Bit-Defender, McAfee, etc. Please disable these programs temporarily to perform the next step. It is also important to remember to re-activate your software firewall after you have completed this step.

Click the "Setup ISP account" button. The Mega 200VWR utility will now open and allow you to enter your ISP(Internet Service Provider) username and password in the fields indicated by the two arrows in Figure 3 and save it to the Mega 200VWR.

✓ Since you have not yet registered/received your VoIP number(s), please leave the VoIP fields as is. You will be given the option to register VoIP account(s) and save them to the router in steps to follow.

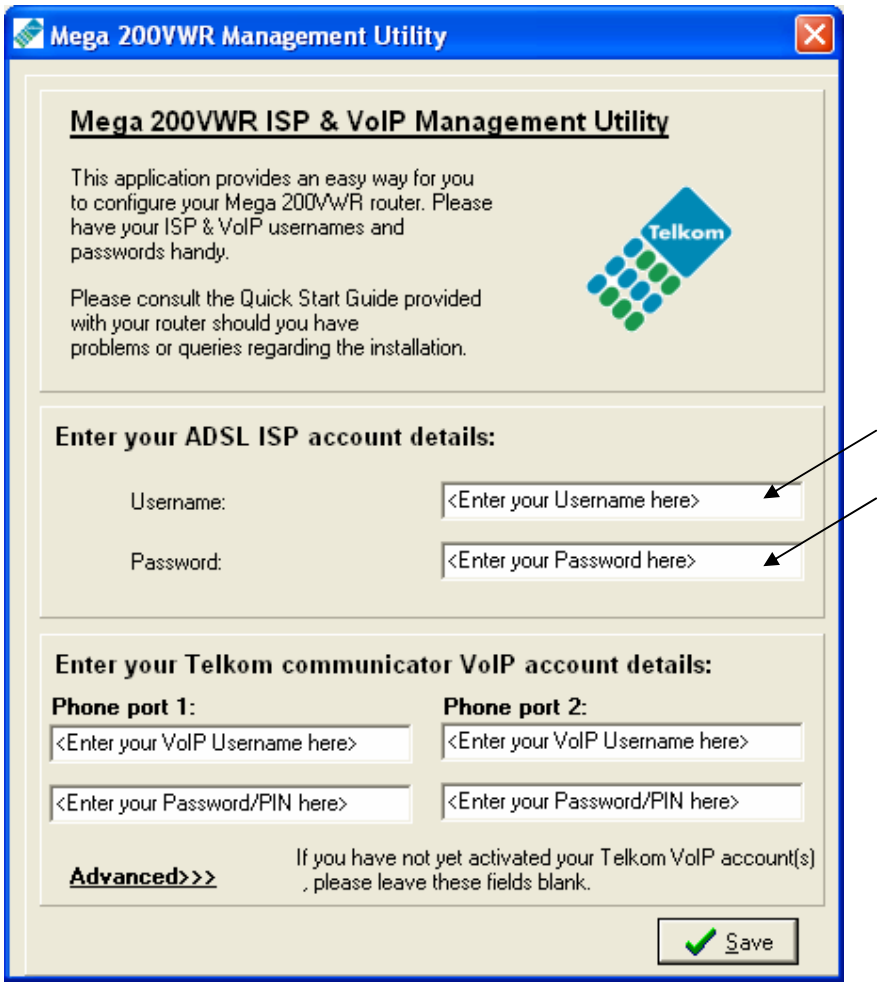


Figure 3

After you have entered your ISP details, click the “Save” button. The router will now be updated with your own ISP account details. On successful completion, a message will be displayed reporting that the save process was a success. Click “Ok” and close the utility , then proceed to the next step.

✓ If the utility does not seem to respond or encounter errors, please refer to error 3 in the troubleshooting section.

✓ If you want to rerun this utility in future, insert the Mega 200VWR CD, then click on “Start”, “Run” and type “D:\ RouterUtil\setup.exe”. Where D is the drive letter representing your CD Rom drive.

4) **Test your Internet connection by opening a webpage:**
Click the 'Test your connection' button. This will open the website www.aardvark.co.za and will serve as a test to determine whether you have performed the previous steps correctly.

If you are able to see aardvark.co.za, please proceed to the next step. If you cannot see the aardvark.co.za webpage, please confirm that you have entered your ISP account details correctly by repeating the previous step. If the problem persists, please contact support.

5) **Setup E-Mail account in Outlook Express: (optional)**
In the step 6 you will register/request a Telkom Internet Communicator VoIP account and on completion of that process the VoIP account details will be e-mailed to you. This step will now assist you in setting up an E-mail account in Outlook Express in order to receive that e-mail.

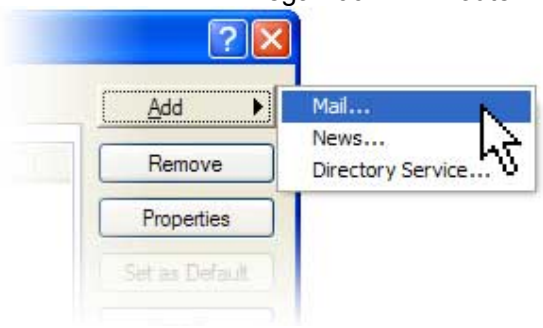
These steps illustrate setting up an E-mail account in Outlook Express. If you prefer to use another mail client application such as Microsoft Office Outlook, please feel free to do so.

Before you continue, ensure that you know your E-mail address, names of the incoming and outgoing mail servers (e.g. pop.telkomsa.net) and your mail account details (usually a pop username and password). Your ISP should have given you this information on a welcome letter of fax. If you do not have this info, please request it from your ISP before you continue.

Please follow steps A - F in order to complete the E-mail account setup:

a. Start Outlook Express by clicking the 'Setup E-Mail account' button on the menu screen or start it manually by selecting it in the programs menu (refer to the figure below). When Outlook Express has opened, click on the **Tools** menu, click **Accounts**. If the Account Setup Wizard starts up automatically, skip ahead to step c.

b. Click Add, and then click Mail.



c. The “Your Name” page will be displayed, type your name as you want it to appear to everyone who gets e-mail from you, then click Next.

d. Enter your E-mail address exactly as provided by your ISP and as you entered it in the Telkom VoIP registration webpage. Click next.

e. Enter your incoming (POP) and outgoing (SMTP) mail server details in the spaces provided. Click next.

f. Enter your account username and password in this form. You will also have the option for Outlook Express to remember your password so that you do not have to retype it every time you download E-mail. Click next and then click finish.

You have now setup your E-mail account and you are ready to receive the E-mail containing your VoIP account details.

6) Register/request VoIP account(s) on the Telkom VoIP website: (optional)

NOTE: ✓ Only Telkom ISP customers qualify for Telkom Internet Communicator VoIP accounts.

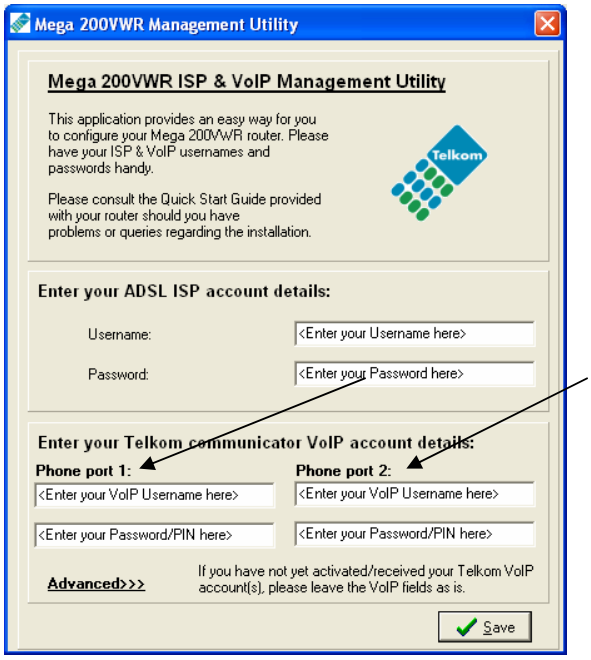
A VoIP account is needed for making cheap Internet voice calls using your Mega 200VWR, much like an ISP account is needed for connecting to the Internet. A VoIP account has two parts, the phone number and password.

Click the ‘Register VoIP Account(s)’ button to open the Telkom VoIP webpage, which will give you the opportunity to register a Telkom Internet Communicator VoIP account. Follow the on-screen instructions.

Once the registration process is complete, your VoIP account details will be e-mailed to the e-mail address specified. You will need these account details to setup VoIP on your Mega 200VWR in the following steps. Please close the VoIP registration page.

7) Setup VoIP account(s) on your Mega 200VWR: (optional)

a. Click the “Setup VoIP accounts” button. The Mega 200VWR Management utility will again open (see figure below).



Important Information

✓ Before you continue, make sure that you do not have any active software firewalls running. These include programs like: Norton Internet Security, TrendMicro’s PC-Cillin, Bit-Defender, McAfee, etc. Please disable these programs temporarily to perform the next step. It is also important to remember to re-activate your software firewall after you have completed this step.

b. Insert the Telkom Internet Communicator VoIP account details you received per e-mail into the spaces provided – indicated by the arrows above. If you have only registered for & received one VoIP account, it is recommended to use the Phone port 1 fields. (More VoIP accounts can be obtained from the Telkom VoIP website, but please be aware that the Mega 200VWR can only accommodate two VoIP accounts at a time.

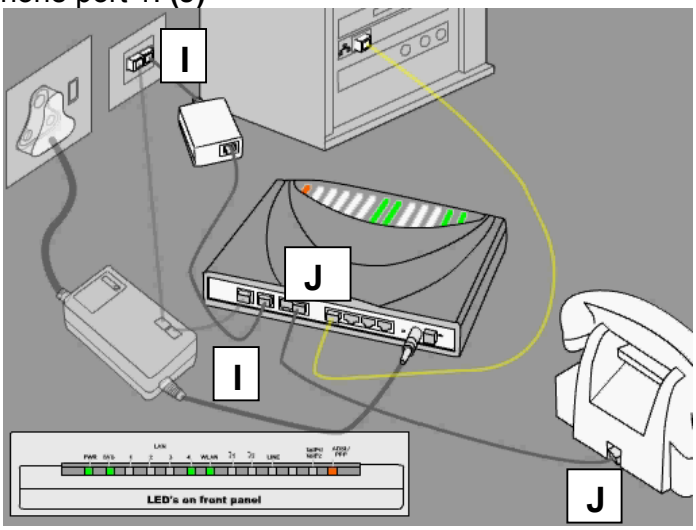
✓ Please also re-insert your ISP details in the top two fields (username and password). This is needed to complete the save action successfully.

c. Click the “Save” button. Your VoIP account and ISP account details will be saved to the router. On successful completion of the process, a message will be displayed. Click ‘Ok’ to close the confirmation message then close the utility by clicking the standard close button (Top-right on the form) returning you to the menu screen.

d. A router restart will be required to initialize your VoIP account(s). Power down the router manually, wait a few seconds and power it up again in order for the new settings to be applied. Once the “ADSL/PPP” LED is steadily lit orange and the VoIP LED is lit, you have successfully saved your VoIP details onto the router.

e. In order to make cost-effective VoIP calls using your standard telephone, you will also need to perform some additional hardware setup tasks. Please follow the two steps below:

- Plug a micro filter into the remaining Telkom ADSL wall-socket and connect the other end of the filter to the “LINE” port on the back panel of your Mega 200VWR, using an enclosed (grey) telephone cable. **(I)**
- Connect the telephones that you intend to use for VoIP to the telephone ports on the back panel of the Mega 200VWR using a telephone cable. Please note that there are two telephone ports and that they correspond to the two VoIP accounts you have seen earlier in this step. If you have only one VoIP account, it is recommended to use telephone port 1. **(J)**



8) Read the router’s user manual:

The last button on the menu, “Read User Manual (.PDF)”, will open the User manual from the CD. It is recommended that you read this manual should you want to make use of some of the advanced features on the Mega 200VWR. The manual is in Adobe Acrobat PDF format and requires Acrobat reader to open the file. If you do not have Acrobat reader installed on your PC. Click on the “Install Acrobat Reader….” hyperlink to the immediate right of the manual button, select your operating system and click install.

NOTE:

✓ You have now completed the Mega 200VWR setup (for Windows 98, 98SE, ME or NT4) and can close the menu screen by clicking the ‘Exit’ button. You should now be able to browse the Internet and make VoIP calls. If you encounter any problems, please refer to the troubleshooting section at the end of the quick start guide and manual or contact the helpdesk.

Mac OS is a registered Trademark of Apple Computer, Inc.
Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered Trademarks of Microsoft Corporation.